(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11212461 A**

(43) Date of publication of application: **06 . 08 . 99**

(51) Int. Cl **G09C 5/00**
G09C 1/00
H04L 9/32
H04N 1/387
H04N 7/08
H04N 7/081

(21) Application number: **10013954**

(22) Date of filing: **27 . 01 . 98**

(71) Applicant: **CANON INC**

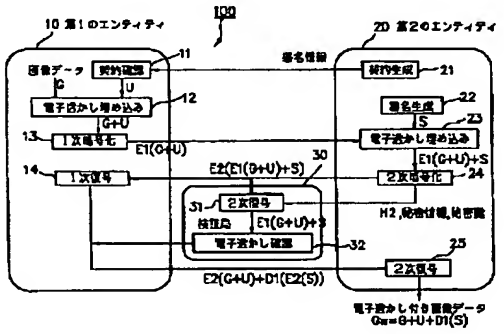
(72) Inventor: **IWAMURA KEIICHI**

(54) **ELECTRONIC WATERMARK SYSTEM AND ELECTRONIC INFORMATION DELIVERY SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an electronic watermark system which surely prevents unauthorized copy of digital data related to copyright.

SOLUTION: The encryption processing and the electronic watermark burying processing of data are distributedly performed in first and second entities (including an author, a selling agent, and a user of data) 10 and 11, and the validity of these encryption processing and electronic watermark burying processing is verified in an independent entity (verification station) 30, thereby surely recognizing the wrong action at the time when the author, the selling agent, or the user wrongfully copies and delivers data. Since check is performed in the verification station in the stage of data delivery from the author to the selling agent and in the stage of that from the selling agent to the user, they cannot do wrong in league with each other, and a system safe against unauthorized delivery of data is realized.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－212461

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	5/00		Ｇ０９Ｃ	5/00	
	1/00	６４０		1/00	６４０Ｃ
Ｈ０４Ｌ	9/32		Ｈ０４Ｎ	1/387	
Ｈ０４Ｎ	1/387		Ｈ０４Ｌ	9/00	６７５Ｄ
	7/08		Ｈ０４Ｎ	7/08	Ｚ

審査請求　未請求　請求項の数30　ＯＬ　（全 24 頁）　最終頁に続く

(21)出願番号　特願平10－13954

(22)出願日　平成10年(1998)１月27日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

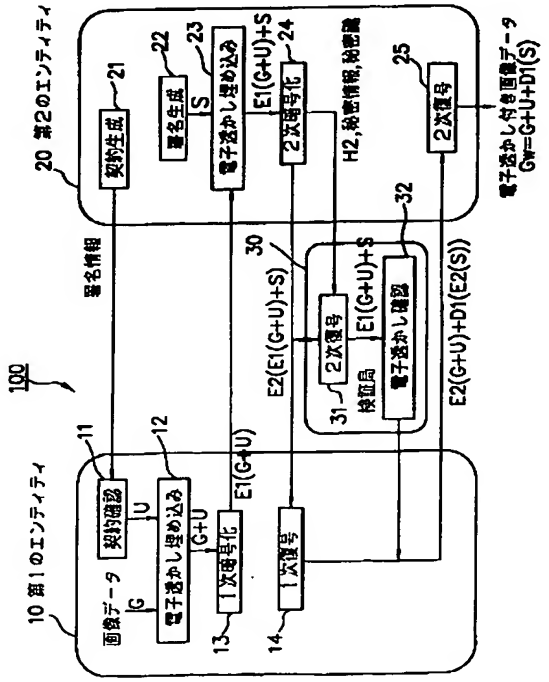
(74)代理人　弁理士　國分　孝悦

(54)【発明の名称】　電子透かし方式および電子情報配布システム

(57)【要約】

【課題】　著作権に係るディジタルデータの不正コピーを確実に防止できる電子透かし方式を提供する。

【解決手段】　データに対する暗号処理および電子透かし埋め込み処理を第１、第２のエンティティ（データの著作者、販売代理店、ユーザを含む）１０，１１で分散して行い、上記暗号処理および電子透かし埋め込み処理の正当性を別個のエンティティ（検証局）３０で検証するようにすることにより、著作者、代理店またはユーザがデータを不正にコピーして配布を行った際にその不正行為を確実に認識することができるようにする。また、このシステムでは、著作者から代理店にデータを渡す段階および代理店からユーザにデータを渡す段階のそれぞれにおいて検証局による検査が行われるので、結託して不正することはあり得ず、データの不正配布に関して安全なシステムを実現できる。



1

【特許請求の範囲】

【請求項１】　データに対する暗号処理および電子透かし埋め込み処理を複数の手段またはエンティティで分散して行い、上記複数の手段またはエンティティで行われた上記暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を、上記複数の手段またはエンティティとは別の手段またはエンティティで検証することを特徴とする電子透かし方式。

【請求項２】　上記複数の手段またはエンティティは、少なくとも３種以上の手段またはエンティティであることを特徴とする請求項１に記載の電子透かし方式。

【請求項３】　上記複数の手段またはエンティティは、データに対して第１の暗号処理を行う手段を有する第１のエンティティと、

上記電子透かし埋め込み処理を行う手段を有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、

第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティとから成ることを特徴とする請求項２に記載の電子透かし方式。

【請求項４】　上記複数の手段またはエンティティは、データに対して第１の暗号処理を行う手段を有する第１のエンティティと、

上記電子透かし埋め込み処理を行う手段を有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、

上記電子透かし埋め込み処理を行う手段および第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティとから成ることを特徴とする請求項２に記載の電子透かし方式。

【請求項５】　上記複数の手段またはエンティティは、データに対して上記電子透かし埋め込み処理を行う手段および第１の暗号処理を行う手段を有する第１のエンティティと、

上記電子透かし埋め込み処理を行う手段を有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、

第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティとから成ることを特徴とする請求項２に記載の電子透かし方式。

【請求項６】　上記複数の手段またはエンティティは、データに対して上記電子透かし埋め込み処理を行う手段および第１の暗号処理を行う手段を有する第１のエンティティと、

上記電子透かし埋め込み処理を行う手段、第１の暗号処理を行う手段および第２の暗号処理を行う手段の少なくとも１つを有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、

上記電子透かし埋め込み処理を行う手段および第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティとから成ることを特徴とする請求項２に記載の電子透かし方式。

2

【請求項７】　上記エンティティは、電子透かしの埋め込まれたデータに対して暗号化を行うことを特徴とする請求項１～６の何れか１項に記載の電子透かし方式。

【請求項８】　上記エンティティは、暗号化の施されたデータに対して電子透かしを埋め込むことを特徴とする請求項１～６の何れか１項に記載の電子透かし方式。

【請求項９】　上記第２のエンティティは、上記第１のエンティティからの上記第１の暗号処理が施されたデータに対して電子透かしを埋め込むことを特徴とする請求項３～６の何れか１項に記載の電子透かし方式。

【請求項１０】　上記第２のエンティティは、上記第１のエンティティからの上記第１の暗号処理が施されたデータおよび上記第３のエンティティからの上記第２の暗号処理が施されたデータに対して電子透かしを埋め込むことを特徴とする請求項３に記載の電子透かし方式。

【請求項１１】　上記第２のエンティティは、上記第２の暗号処理が施されたデータを一方向性関数により変換した値を出力することを特徴とする請求項１０に記載の電子透かし方式。

【請求項１２】　上記第２のエンティティは、上記一方向性関数により変換した値を上記第４のエンティティに送信することを特徴とする請求項１１に記載の電子透かし方式。

【請求項１３】　上記第３のエンティティは、上記第２の暗号処理が施されたデータを一方向性関数により変換した値を上記第２の暗号処理が施されたデータと共に出力することを特徴とする請求項３～６の何れか１項に記載の電子透かし方式。

【請求項１４】　上記第３のエンティティは、上記一方向性関数により変換した値を上記第４のエンティティに送信することを特徴とする請求項１３に記載の電子透かし方式。

【請求項１５】　上記第３のエンティティは、あらかじめ一次暗号化された情報を受け取り、該暗号化された情報に対して二次暗号化を施すことを特徴とする請求項３～６の何れか１項に記載の電子透かし方式。

【請求項１６】　上記第４のエンティティは、上記第２の暗号処理に対応する復号処理を行うことが可能であることを特徴とする請求項３～６の何れか１項に記載の電子透かし方式。

【請求項１７】　上記第４のエンティティは、暗号鍵を管理する手段を有することを特徴とする請求項３～６の何れか１項に記載の電子透かし方式。

【請求項１８】　上記第４のエンティティは、他のエンティティから出力される暗号化され電子透かしが埋め込まれたデータを復号化することにより、上記電子透かしおよび暗号処理の少なくとも一方の正当性を検証することを特徴とする請求項１７に記載の電子透かし方式。

【請求項１９】　上記第４のエンティティは、上記他のエンティティから出力される暗号化され電子透かしが埋め込まれたデータを一方向性関数で変換した値と、上記他のエンティティから出力される値とを比較することにより、上記電子透かしおよび暗号処理の少なくとも一方の正当性を検証することを特徴とする請求項１７または１８に記載の電子透かし方式。

【請求項２０】　複数のエンティティからなるネットワークシステム上でディジタルデータの送受信を行う電子情報配布システムにおいて、
データに対して第１の暗号処理を行う手段を有する第１のエンティティと、
電子透かし埋め込み処理を行う手段を有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、
第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティと、
上記第１～第３のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第４のエンティティとを有することを特徴とする電子情報配付システム。

【請求項２１】　複数のエンティティからなるネットワークシステム上でディジタルデータの送受信を行う電子情報配布システムにおいて、
データに対して第１の暗号処理を行う手段を有する第１のエンティティと、
電子透かし埋め込み処理を行う手段を有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、
上記電子透かし埋め込み処理を行う手段および第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティと、
上記第１～第３のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第４のエンティティとを有することを特徴とする電子情報配付システム。

【請求項２２】　複数のエンティティからなるネットワークシステム上でディジタルデータの送受信を行う電子情報配布システムにおいて、
データに対して電子透かし埋め込み処理を行う手段および第１の暗号処理を行う手段を有する第１のエンティティと、
上記電子透かし埋め込み処理を行う手段を有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、
第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティと、
上記第１～第３のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第４のエンティティとを有することを特徴とする電子情報配付システム。

【請求項２３】　複数のエンティティからなるネットワークシステム上でディジタルデータの送受信を行う電子情報配布システムにおいて、
データに対して電子透かし埋め込み処理を行う手段および第１の暗号処理を行う手段を有する第１のエンティティと、
上記電子透かし埋め込み処理を行う手段、第１の暗号処理を行う手段および第２の暗号処理を行う手段の少なくとも１つを有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、
上記電子透かし埋め込み処理を行う手段および第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティと、
上記第１～第３のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第４のエンティティとを有することを特徴とする電子情報配付システム。

【請求項２４】　上記検証を行う第４のエンティティは、暗号鍵を管理するエンティティであることを特徴とする請求項２０～２３の何れか１項に記載の電子情報配布システム。

【請求項２５】　上記第１のエンティティが埋め込む電子透かし情報は、上記第３のエンティティに関する情報を含むことを特徴とする請求項２２または２３に記載の電子情報配布システム。

【請求項２６】　上記第１のエンティティが埋め込む電子透かし情報は、送信するディジタルデータに関する情報を含むことを特徴とする請求項２２または２３に記載の電子情報配布システム。

【請求項２７】　上記第２のエンティティが埋め込む電子透かし情報は、上記第３のエンティティに関する情報を含むことを特徴とする請求項２０～２３の何れか１項に記載の電子情報配布システム。

【請求項２８】　上記第３のエンティティが埋め込む電子透かし情報は、上記第３のエンティティのみが作成できる情報であることを特徴とする請求項２１または２３に記載の電子情報配布システム。

【請求項２９】　上記第１のエンティティは、認証局によって発行される証明書付匿名公開鍵によって上記第３のエンティティの署名を検証した後に上記電子透かし埋め込み処理を行うことを特徴とする請求項２２または２３に記載の電子情報配布システム。

【請求項３０】　上記第２のエンティティは、認証局によって発行される証明書付匿名公開鍵によって上記第３のエンティティの署名を検証した後に上記電子透かし埋め込み処理を行うことを特徴とする請求項２０～２３の何れか１項に記載の電子情報配布システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は電子透かし方式および電子情報配布システムに関し、特に、動画像データ、静止画像データ、音声データ、コンピュータデータ、コンピュータプログラム等のディジタル情報における著作権を保護するための電子透かし技術、およびそれを用いてディジタル情報の配布を行うマルチメディアネットワークに用いて好適なものである。

【０００２】

【従来の技術】近年のコンピュータネットワークの発達と、安価で高性能なコンピュータの普及とにより、ネットワーク上で商品の売買を行う電子商取引が盛んになってきている。そこで取引される商品として、例えば画像等を含むディジタルデータが考えられる。しかし、ディジタルデータは、完全なコピーを容易かつ大量に作成できるという性質を持ち、これは、そのディジタルデータを買ったユーザがオリジナルと同質のコピーを不正に作成して再配布できるという可能性を示す。これにより、本来ディジタルデータの著作者または著作者から正当に販売を委託された者（以下、「販売者」と言う）に支払われるべき代価が支払われず、著作権が侵害されていると考えられる。

【０００３】一方、著作者または販売者（以下、これらのディジタルデータを正当に配布する者をまとめて「サーバ」と言う）がユーザにディジタルデータを一度送ってしまうと、上述の不正コピーを完全に防止することはできない。そのため、不正コピーを直接防止するのではなく、電子透かしと呼ばれる手法が提案されている。この電子透かしとは、オリジナルのディジタルデータにある操作を加え、ディジタルデータに関する著作権情報やユーザに関する利用者情報をディジタルデータ中に埋め込むことによって、不正コピーが見つかった場合に誰がデータを再配布したのかを特定する手法である。

【０００４】従来の電子透かしを用いたシステムでは、サーバは完全に信頼できる機関であることが前提となっている。よって、もしサーバが信頼できる機関ではなく不正を行う可能性があるとすると、従来のシステムでは不正コピーを行っていないユーザに罪が押し付けられてしまう場合が存在する。

【０００５】これは、図１３に示すように、従来のシステムでは、ユーザを特定するための利用者情報ｄ１をディジタルデータ（以下、ディジタルデータを画像データとして説明する）ｇにサーバが埋め込むので、サーバが勝手に利用者情報ｄ１を埋め込んでそのコピーを不正に配布した場合、その利用者情報ｄ１から特定されるユーザは、サーバの主張を退ける手段がないためである。

【０００６】その対策として、例えば、「B.Pfitmann and M.Waidner：“Asymmetic Fingerprinting,”EUROCRYPT'96」の文献（以下、文献[1]と記す）に、公開鍵暗号方式を用いたシステム（図１４）が提案されている。ここで、公開鍵暗号方式とは、暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。その代表例として、ＲＳＡ暗号やＥ１Ｇａｍａ１暗号等が知られている。以下、公開鍵暗号方式における（ａ）特徴、（ｂ）秘密通信や認証通信等のプロトコルについて述べる。

【０００７】（ａ）公開鍵暗号の特徴

（１）暗号鍵と復号鍵とが異なり、暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

（２）各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよい。

（３）送られてきた通信文の送信者が偽者でないこと、およびその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【０００８】（ｂ）公開鍵暗号のプロトコル

例えば、通信文Ｍに対して、公開の暗号鍵ｋｐを用いて行う暗号化操作をＥ（ｋｐ，Ｍ）とし、秘密の復号鍵ｋｓを用いて行う復号操作をＤ（ｋｓ，Ｍ）とすると、公開鍵暗号アルゴリズムは、まず次の２つの条件を満たす。

（１）暗号鍵ｋｐが与えられたとき、暗号化操作Ｅ（ｋｐ，Ｍ）の計算は容易である。また、復号鍵ｋｓが与えられたとき、復号操作Ｄ（ｋｓ，Ｍ）の計算は容易である。

（２）もしユーザが復号鍵ｋｓを知らないなら、暗号鍵ｋｐと、暗号化操作Ｅ（ｋｐ，Ｍ）の計算手順と、暗号文Ｃ＝Ｅ（ｋｐ，Ｍ）とを知っていても、通信文Ｍを決定することは計算量の点で困難である。

【０００９】次に、上記（１）、（２）の条件に加えて、次の（３）の条件が成立することにより秘密通信機能が実現できる。

（３）全ての通信文（平文）Ｍに対し暗号化操作Ｅ（ｋ，，Ｍ）が定義でき、

Ｄ（ｋｓ，Ｅ（ｋｐ，Ｍ））＝Ｍ

が成立する。つまり、暗号鍵ｋｐは公開されているため、誰もが暗号化操作Ｅ（ｋｐ，Ｍ）の計算を行うことができるが、Ｄ（ｋｓ，Ｅ（ｋｐ，Ｍ））の計算をして通信文Ｍを得ることができるのは、秘密の復号鍵ｋｓを持っている本人だけである。

【００１０】一方、上記（１）、（２）の条件に加えて、次の（４）の条件が成立することにより認証通信機能が実現できる。

（４）全ての通信文（平文）Ｍに対し復号操作Ｄ（ｋｓ，Ｍ）が定義でき、

Ｅ（ｋｐ，Ｄ（ｋｓ，Ｍ））＝Ｍ

が成立する。つまり、復号操作Ｄ（ｋｓ，Ｍ）の計算ができるのは秘密の復号鍵ｋｓを持っている本人のみであり、他の人が偽の秘密の復号鍵ｋｓ’を用いてＤ（ｋｓ’，Ｍ）の計算を行い、秘密の復号鍵ｋｓを持っている本人になりすましたとしても、

Ｅ（ｋｐ，Ｄ（ｋｓ’，Ｍ）≠Ｍ
であるため、受信者は受けとった情報が不正なものであることを確認できる。また、Ｄ（ｋｓ，Ｍ）の値が改ざんされても、
Ｅ（ｋｐ，Ｄ（ｋｓ，Ｍ）’）≠Ｍ
となり、受信者は受けとった情報が不正なものであることを確認できる。

【００１１】上述のような公開鍵暗号方式では、公開の暗号鍵（以下、公開鍵とも言う）ｋｐを用いる処理Ｅ()を「暗号化」、秘密の復号鍵（以下、秘密鍵とも言う）ｋｓを用いる処理Ｄ()を「復号」と呼んでいる。したがって、秘密通信では送信者が暗号化を行い、その後受信者が復号を行うが、認証通信では送信者が復号を行い、その後受信者が暗号化を行うことになる。

【００１２】以下に、公開鍵暗号方式により送信者Ａから受信者Ｂへ秘密通信、認証通信、署名付秘密通信を行う場合のプロトコルを示す。ここで、送信者Ａの秘密鍵をｋｓＡ、公開鍵をｋｐＡとし、受信者Ｂの秘密鍵をｋｓＢ、公開鍵をｋｐＢとする。

【００１３】[秘密通信]送信者Ａから受信者Ｂへ通信文（平文）Ｍを秘密通信する場合は、次の手順で行う。
Ｓｔｅｐ１：送信者Ａは、受信者Ｂの公開鍵ｋｐＢで通信文Ｍを以下のように暗号化し、暗号文Ｃを受信者Ｂに送る。
Ｃ＝Ｅ（ｋｐＢ，Ｍ）
Ｓｔｅｐ２：受信者Ｂは、自分の秘密鍵ｋｓＢで暗号文Ｃを以下のように復号し、もとの平文Ｍを得る。
Ｍ＝Ｄ（ｋｓＢ，Ｃ）
なお、受信者Ｂの公開鍵ｋｐＢは不特定多数に公開されているので、送信者Ａに限らず全ての人が受信者Ｂに秘密通信できる。

【００１４】[認証通信]送信者Ａから受信者Ｂへ通信文（平文）Ｍを認証通信する場合は、次の手順で行う。
Ｓｔｅｐ１：送信者Ａは、自分の秘密鍵ｋｓＡで送信文Ｓを以下のように生成し、受信者Ｂに送る。
Ｓ＝Ｄ（ｋｓＡ，Ｍ）
この送信文Ｓを「署名文」と言い、署名文Ｓを得る操作を「署名」と言う。
Ｓｔｅｐ２：受信者Ｂは、送信者Ａの公開鍵ｋｐＡで署名文Ｓを以下のように復元変換し、もとの平文Ｍを得る。
Ｍ＝Ｅ（ｋｐＡ，Ｓ）
もし、通信文Ｍが意味のある文であることを確認したならば、通信文Ｍが確かに送信者Ａから送られてきたことを認証する。送信者Ａの公開鍵ｋｐＡは不特定多数に公開されているので、受信者Ｂに限らず全ての人が送信者Ａの署名文Ｓを認証できる。このような認証を「ディジタル署名」とも言う。

【００１５】[署名付秘密通信]送信者Ａから受信者Ｂへ通信文（平文）Ｍを署名付秘密通信する場合は、次の手順で行う。
Ｓｔｅｐ１：送信者Ａは、自分の秘密鍵ｋｓＡで通信文Ｍを以下のように署名し、署名文Ｓを作る。
Ｓ＝Ｄ（ｋｓＡ，Ｍ）
さらに、送信者Ａは、受信者Ｂの公開鍵ｋｐＢで署名文Ｓを以下のように暗号化し、暗号文Ｃを受信者Ｂに送る。
Ｃ＝Ｅ（ｋｐＢ，Ｓ）
Ｓｔｅｐ２：受信者Ｂは、自分の秘密鍵ｋｓＢで暗号文Ｃを以下のように復号し、署名文Ｓを得る。
Ｓ＝Ｄ（ｋｓＢ，Ｃ）
さらに、受信者Ｂは、送信者Ａの公開鍵ｋｐＡで署名文Ｓを以下のように復元変換し、もとの平文Ｍを得る。
Ｍ＝Ｅ（ｋｐＡ，Ｓ）
もし、通信文Ｍが意味のある文であることを確認したならば、通信文Ｍが確かに送信者Ａから送られてきたことを認証する。

【００１６】なお、署名付秘密通信の各Ｓｔｅｐ内における関数を施す順序は、それぞれ逆転しても良い。すなわち、上述の手順では、
Ｓｔｅｐ１：Ｃ＝Ｅ（ｋｐＢ，Ｄ（ｋｓＡ，Ｍ））
Ｓｔｅｐ２：Ｍ＝Ｅ（ｋｐＡ，Ｄ（ｋｓＢ，Ｃ））
となっているが、下記のような手順でも署名付秘密通信が実現できる。
Ｓｔｅｐ１：Ｃ＝Ｄ（ｋｓＡ，Ｅ（ｋｐＢ，Ｍ））
Ｓｔｅｐ２：Ｍ＝Ｄ（ｋｓＢ，Ｅ（ｋｐＡ，Ｃ））

【００１７】以下に、上述のような公開鍵暗号方式を適用した従来の電子透かしを用いるシステム（上記図１４）における操作の手順を示す。
１）まず、サーバとユーザ間で画像データｇの売買に関する契約書ｄ２を取り交わす。

【００１８】２）次に、ユーザは、自分を示す乱数ＩＤを発生させ、これを用いて一方向性関数ｆを生成する。この一方向性関数とは、関数ｙ＝ｆ（ｘ）において、ｘからｙを求めることは容易だが、逆にｙからｘを求めることが困難な関数を言う。例えば、桁数の大きな整数に対する素因数分解や離散的対数等が一方向性関数としてよく用いられる。
３）次に、ユーザは、契約書ｄ２と一方向性関数ｆに対して、自分の秘密鍵ｋｓＵを用いて署名情報ｄ３を生成し、それらを合わせてサーバに送る。

【００１９】４）次に、サーバは、ユーザの公開鍵ｋｐＵを用いて署名情報ｄ３と契約書ｄ２を確認する。
５）サーバは確認後、現在までの全配布記録ｄ４と、ユーザが作成した乱数ＩＤとを画像データｇに埋め込み、電子透かし付き画像データ（ｇ＋ｄ４＋ＩＤ）を生成する。
６）サーバは、ユーザにその電子透かし付き画像データ（ｇ＋ｄ４＋ＩＤ）を送る。

【００２０】この後、不正コピーが発見された場合は、その不正画像データから埋め込み情報を抽出し、そこに

含まれるＩＤからユーザを特定する。このとき、その不正コピーがサーバによって無断で配布されたものでないことは、以下のことを根拠として主張される。それは、ユーザを特定するＩＤはユーザ自身によって生成され、それを用いた一方向性関数値ｆにユーザの署名が付けられるので、サーバは任意のユーザに対してそのようなＩＤを生成できないということである。しかし、サーバとの間で正式に契約したユーザは自分を特定するＩＤをサーバに送るために、正式に契約したユーザへの罪の押し付けはやはり可能であり、契約していないユーザへの罪の押し付けが不可能になるだけである。

【００２１】そこで、正式に契約したユーザにも罪の押し付けが不可能になるシステム（図１５）が、「三浦，渡辺，嵩（奈良先端大）：“サーバの不正も考慮した電子透かしについて”，SCIS97-31C」の文献（以下、文献[2]と記す）に提案されている。これは、サーバを原画像サーバと埋め込みサーバに分割することによって実現される。ただし、このシステムでは、暗号化時および復号時において、埋め込まれた電子透かしは壊されないとしている。以下、上記図１５のシステムにおける操作の手順を示す。

【００２２】１）まず、ユーザが原画像サーバに所望の画像データを、署名ｄ５を付けて要求する。

２）原画像サーバは、その要求内容をユーザの署名ｄ５から確認し、その確認後に、要求された画像データｇを暗号化して埋め込みサーバに送る。このとき、原画像サーバは、ユーザ名ｕおよび委託内容ｄ６に対する署名を付けて埋め込みサーバに送る。これと同時に、原画像サーバは、暗号化に対する復号関数ｆ’をユーザに送る。

【００２３】３）埋め込みサーバは、送られてきた暗号化画像データｇ’と、署名（ｕ＋ｄ６）とを確認し、ユーザ名ｕおよび委託内容ｄ６を基にユーザを特定する利用者情報ｄ７の作成および埋め込みを行い、電子透かし付き暗号化画像データ（ｇ’＋ｄ７）を作成する。その後、埋め込みサーバは、その電子透かし付き暗号化画像データ（ｇ’＋ｄ７）をユーザに送る。

４）ユーザは、原画像サーバから送られてきた復号関数ｆ’を用いて、電子透かし付き暗号化画像データ（ｇ’＋ｄ７）を電子透かし付き画像データ（ｇ＋ｄ７）へと復号する。

【００２４】この後、不正コピーが発見された場合は、原画像サーバはその不正画像データを暗号化して埋め込み情報を抽出し、それを埋め込みサーバに送る。埋め込みサーバは、この埋め込み情報からユーザを特定する。このシステムでは、原画像サーバはユーザを特定するための利用者情報ｄ７を画像データｇに埋め込んでおらず、また、埋め込みサーバは復号関数ｆ’を知らない（画像を元に戻せない）ので、正式に契約したユーザに対しても、各サーバはユーザの利用者情報ｄ７を無断で埋め込んだ画像データを不正配布できないことを根拠にしている。

【００２５】しかしながら、この図１５のシステムでは、原画像サーバと埋め込みサーバとの結託については考慮せず、埋め込みサーバとユーザとの結託も考えていない。よって、埋め込みサーバが原画像である画像データｇの暗号化画像データｇ’を持ち、ユーザが復号関数ｆ’を持つため、原画像サーバと埋め込みサーバとが結託した場合には、上述の図１４のシステムと同様にサーバの不正が可能であるし、埋め込みサーバとユーザとが結託した場合には原画像の不正入手が可能である。

【００２６】また、原画像サーバは復号関数ｆ’をユーザに送るが、ユーザの復号関数ｆ’の管理が不十分であれば、埋め込みサーバはユーザと結託しなくてもユーザの不注意等から復号関数ｆ’を知ることができる可能性は大きい。

【００２７】さらに、このシステムでは、原画像サーバは埋め込み手段を有しない、または正しい埋め込みができないとしているが、埋め込み情報を抽出するのは原画像サーバであるので、埋め込み情報を解析すれば、原画像サーバが正しい埋め込みを行えるようになる可能性は高いと考えられる。そして、この場合、上述の図１４のシステムと同様の不正が可能である。

【００２８】さらに、上述のように従来はユーザとサーバとからなるシステムが不完全ながら提案されていたが、画像データの売買に関係する要素が階層的に構成される場合における安全なシステムは提案されていなかった。階層的なシステムの例としては、図１６に示すように、サーバの下に複数の代理店があり、その下にユーザがあるといったシステムであったり、図１７に示すように、ある販売代理店に複数の著作者が自分の著作に係る画像データの販売を依頼し、その依頼を受けた代理店が複数の著作者の画像データを多くのユーザに販売するといったシステムとして考えられる。

【００２９】これらの階層的なシステムにおいては、画像データの売買を構成する要素が上述のサーバおよびユーザの二者からサーバ（または著作者）、代理店およびユーザの三者に増えるために、結託の問題などは構成要素が二者のシステムよりも複雑になる。すなわち、上記図１５のシステムは広く考えると、サーバと代理店とユーザとが構成要素のシステムであるとも考えられるが、文献[2]は階層的なシステムを想定したものではなく、１つのサーバの不正を防止するという観点からサーバを分割したものであり、上述のように結託の問題も考慮していない。

【００３０】

【発明が解決しようとする課題】本発明はこのような実情に鑑みて成されたものであり、上述のような不正を確実に防止できる電子透かし方式および電子情報配布システムを提供することを目的とする。特に本発明は、著作物の売買に関係する要素が階層的に構成されているシス

テムにおいて、結託による不正を確実に防止できるようにすることを目的としている。

【００３１】

【課題を解決するための手段】本発明の電子透かし方式は、データに対する暗号処理および電子透かし埋め込み処理を複数の手段またはエンティティで分散して行い、上記複数の手段またはエンティティで行われた上記暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を、上記複数の手段またはエンティティとは別の手段またはエンティティで検証することを特徴とする。ここで、上記複数の手段またはエンティティは、少なくとも３種以上の手段またはエンティティであっても良い。

【００３２】例えば、上記複数の手段またはエンティティは、データに対して第１の暗号処理を行う手段を有する第１のエンティティと、上記電子透かし埋め込み処理を行う手段を有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティとから成るものであっても良い。

【００３３】また、上記複数の手段またはエンティティは、データに対して第１の暗号処理を行う手段を有する第１のエンティティと、上記電子透かし埋め込み処理を行う手段を有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、上記電子透かし埋め込み処理を行う手段および第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティとから成るものであっても良い。

【００３４】また、上記複数の手段またはエンティティは、データに対して上記電子透かし埋め込み処理を行う手段および第１の暗号処理を行う手段を有する第１のエンティティと、上記電子透かし埋め込み処理を行う手段を有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティとから成るものであっても良い。

【００３５】さらに、上記複数の手段またはエンティティは、データに対して上記電子透かし埋め込み処理を行う手段および第１の暗号処理を行う手段を有する第１のエンティティと、上記電子透かし埋め込み処理を行う手段、第１の暗号処理を行う手段および第２の暗号処理を行う手段の少なくとも１つを有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、上記電子透かし埋め込み処理を行う手段および第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティとから成るものであっても良い。

【００３６】上記の構成において、上記エンティティは、電子透かしの埋め込まれたデータに対して暗号化を行うようにしても良い。また、上記エンティティは、暗号化の施されたデータに対して電子透かしを埋め込むようにしても良い。

【００３７】また、上記第２のエンティティは、上記第１のエンティティからの上記第１の暗号処理が施されたデータに対して電子透かしを埋め込むようにしても良い。また、上記第２のエンティティは、上記第１のエンティティからの上記第１の暗号処理が施されたデータおよび上記第３のエンティティからの上記第２の暗号処理が施されたデータに対して電子透かしを埋め込むようにしても良い。また、上記第２のエンティティは、上記第２の暗号処理が施されたデータを一方向性関数により変換した値を出力するようにしても良い。また、上記第２のエンティティは、上記一方向性関数により変換した値を上記第４のエンティティに送信するようにしても良い。

【００３８】また、上記第３のエンティティは、上記第２の暗号処理が施されたデータを一方向性関数により変換した値を上記第２の暗号処理が施されたデータと共に出力するようにしても良い。また、上記第３のエンティティは、上記一方向性関数により変換した値を上記第４のエンティティに送信するようにしても良い。また、上記第３のエンティティは、あらかじめ一次暗号化された情報を受け取り、該暗号化された情報に対して二次暗号化を施すようにしても良い。

【００３９】また、上記第４のエンティティは、上記第２の暗号処理に対応する復号処理を行うことが可能であるようにしても良い。また、上記第４のエンティティは、暗号鍵を管理する手段を有するようにしても良い。また、上記第４のエンティティは、他のエンティティから出力される暗号化され電子透かしが埋め込まれたデータを復号化することにより、上記電子透かしおよび暗号処理の少なくとも一方の正当性を検証するようにしても良い。また、上記第４のエンティティは、上記他のエンティティから出力される暗号化され電子透かしが埋め込まれたデータを一方向性関数で変換した値と、上記他のエンティティから出力される値とを比較することにより、上記電子透かしおよび暗号処理の少なくとも一方の正当性を検証するようにしても良い。

【００４０】また、本発明の電子情報配布システムは、複数のエンティティからなるネットワークシステム上でディジタルデータの送受信を行う電子情報配布システムにおいて、データに対して第１の暗号処理を行う手段を有する第１のエンティティと、電子透かし埋め込み処理を行う手段を有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティと、上記第１～第３のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第４のエンティ

ティとを有することを特徴とする。

【００４１】本発明の他の態様では、複数のエンティティからなるネットワークシステム上でディジタルデータの送受信を行う電子情報配布システムにおいて、データに対して第１の暗号処理を行う手段を有する第１のエンティティと、電子透かし埋め込み処理を行う手段を有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、上記電子透かし埋め込み処理を行う手段および第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティと、上記第１～第３のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第４のエンティティとを有することを特徴とする。

【００４２】本発明のその他の態様では、複数のエンティティからなるネットワークシステム上でディジタルデータの送受信を行う電子情報配布システムにおいて、データに対して電子透かし埋め込み処理を行う手段および第１の暗号処理を行う手段を有する第１のエンティティと、上記電子透かし埋め込み処理を行う手段を有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティと、上記第１～第３のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第４のエンティティとを有することを特徴とする。

【００４３】本発明のその他の態様では、複数のエンティティからなるネットワークシステム上でディジタルデータの送受信を行う電子情報配布システムにおいて、データに対して電子透かし埋め込み処理を行う手段および第１の暗号処理を行う手段を有する第１のエンティティと、上記電子透かし埋め込み処理を行う手段、第１の暗号処理を行う手段および第２の暗号処理を行う手段の少なくとも１つを有し、上記第１のエンティティからのデータを管理および配付する第２のエンティティと、上記電子透かし埋め込み処理を行う手段および第２の暗号処理を行う手段を有し、電子透かし付きデータを利用する第３のエンティティと、上記第１～第３のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第４のエンティティとを有することを特徴とする。

【００４４】ここで、上記検証を行う第４のエンティティは、暗号鍵を管理するエンティティであっても良い。また、上記第１のエンティティが埋め込む電子透かし情報は、上記第３のエンティティに関する情報を含んでも良い。また、上記第１のエンティティが埋め込む電子透かし情報は、送信するディジタルデータに関する情報を含んでも良い。また、上記第２のエンティティが埋め込む電子透かし情報は、上記第３のエンティティに関する情報を含んでも良い。また、上記第３のエンティティが埋め込む電子透かし情報は、上記第３のエンティティのみが作成できる情報であっても良い。また、上記第１のエンティティは、認証局によって発行される証明書付匿名公開鍵によって上記第３のエンティティの署名を検証した後に上記電子透かし埋め込み処理を行うようにしても良い。また、上記第２のエンティティは、認証局によって発行される証明書付匿名公開鍵によって上記第３のエンティティの署名を検証した後に上記電子透かし埋め込み処理を行うようにしても良い。

【００４５】

【発明の実施の形態】〔第１の実施形態〕以下、本発明に係る第１の実施形態を、図１を参照して説明する。本発明に係る電子透かし方式は、例えば、図１に示すようなシステム１００により実施され、このシステム１００は、本発明に係る電子情報配布システムを適用したものでもある。

【００４６】すなわち、システム１００は、第１のエンティティ側の端末装置（以下、第１端末装置と記す）１０、第２のエンティティ側の端末装置（以下、第２端末装置と記す）２０および検証局側の端末装置（以下、検証局端末装置と記す）３０を含む多数のエンティティ（図示せず）からなるネットワークシステムであり、各エンティティは、ネットワークを介して互いにディジタルデータの授受を行うようになされている。

【００４７】第１端末装置１０は、第２端末装置２０からのデータが供給される契約確認処理部１１と、例えば画像データ（ディジタルデータ）および契約確認処理部１１の出力が供給される電子透かし埋め込み処理部１２と、電子透かし埋め込み処理部１２の出力が供給される１次暗号化処理部１３と、第２端末装置２０からのデータが供給される１次復号処理部１４とを備えており、１次暗号化処理部１３および１次復号処理部１４の各出力が第２端末装置２０に送信されるようになされている。

【００４８】また、第２端末装置２０は、第１端末装置１０の契約確認処理部１１に対してデータを送信する契約生成処理部２１と、署名生成処理部２２と、署名生成処理部２２および第１端末装置１０の１次暗号化処理部１３からのデータが供給される電子透かし埋め込み処理部２３と、電子透かし埋め込み処理部２３の出力が供給される２次暗号化処理部２４と、第１端末装置１０の１次復号処理部１４からのデータが供給される２次復号処理部２５とを備えており、２次復号処理部２５の出力が電子透かし付き画像データとして出力されるようになされている。また、２次暗号化処理部２４の出力は、第１端末装置１０の１次復号処理部１４および検証局端末装置３０に各々供給されるようになされている。

【００４９】また、検証局端末装置３０は、第２端末装置２０の２次暗号化処理部２４からのデータが供給される２次復号処理部３１と、２次復号処理部３１の出力が

供給される電子透かし確認処理部３２とを備えており、電子透かし確認処理部３２の出力が第１端末装置１０と第２端末装置２０とに供給されるようになされている。また、２次復号処理部３１の出力は、第１端末装置１０の１次復号処理部１４にも供給されるようになされている。

【００５０】上記のように構成された本実施形態の電子情報配布システムにおいて、以下では、図１６または図１７に示したサーバまたは著作者が代理店にディジタルデータを渡す際の第１の埋込処理と、代理店がユーザにディジタルデータを渡す際の第２の埋込処理とに分けて考える。本実施形態は、第１の埋込処理と第２の埋込処理とを下記に示す同じプロトコルを用いて実現する。全体の処理は、第１の埋込処理を行った後に第２の埋込処理を行う。

【００５１】下記の説明において、第１の埋込処理では上述の第１のエンティティはサーバまたは著作者を意味し、第２のエンティティは代理店を意味する。また、第２の埋込処理では第１のエンティティは代理店を意味し、第２のエンティティはユーザを意味する。したがって、少なくとも代理店において使用する端末装置は、図１の第１端末装置１０と第２端末装置２０に備えられた各処理部を全て有するものである。

【００５２】上記第１の埋込処理および第２の埋込処理を実現する具体的なプロトコルを、図１を参照しながら以下に説明する。このプロトコルにおいて、方式や秘密鍵等の１次暗号に関する情報は第１のエンティティだけが知る情報であり、２次暗号に関する情報は第２のエンティティだけが知る情報である。ただし、これらの暗号の間には、どちらの暗号化を先に行っても復号を行うとその暗号は解かれる、という性質を持つものとする。以下、暗号化を「Ｅｉ（）」、復号を「Ｄｉ（）」で表わし、電子透かしに関する埋め込み処理を「＋」で表わすものとする。

【００５３】以下に、上記のように構成したシステム１００の動作を説明する。まず、電子透かしに関する埋め込み処理について説明する。

【００５４】[埋め込み処理]

１）まず、第２端末装置２０において、第２のエンティティが署名を付けて第１端末装置１０（第１のエンティティ）に所望の画像データを要求する。この要求データは、契約生成処理部２１により生成された署名情報であり、以下ではこれを契約情報と呼ぶ。

【００５５】２）次に、第１端末装置１０において第１のエンティティは、契約確認処理部１１を用いて受信した契約情報を第２のエンティティの署名から確認し、その確認後に、契約情報から利用者情報Ｕを作成する。そして、電子透かし埋め込み処理部１２は、上記契約確認処理部１１で作成された利用者情報Ｕを要求された画像データＧに埋め込む。また、１次暗号化処理部１３は、電子透かし埋込処理部１２で利用者情報Ｕが埋め込まれた画像データ（Ｇ＋Ｕ）に対して１次暗号化処理Ｅ１()を行い、得られたデータを第２端末装置２０に送る。よって、第２端末装置２０には、１次暗号化画像データＥ１（Ｇ＋Ｕ）の情報が送られることになる。

【００５６】３）次に、第２端末装置２０において、署名生成処理部２２は、第２のエンティティの秘密鍵を用いて署名情報Ｓを生成する。そして、電子透かし埋め込み処理部２３は、署名生成処理部２２で生成された署名情報Ｓを、第１端末装置１０から送られてきた（配布された）１次暗号化画像データＥ１（Ｇ＋Ｕ）に埋め込む。また、２次暗号化処理部２４は、電子透かし埋め込み処理部２３で署名情報Ｓが埋め込まれた１次暗号化画像データＥ１（Ｇ＋Ｕ）＋Ｓを２次暗号化して検証局端末装置３０に送る。よって、検証局端末装置３０には、２次暗号化画像データＥ２（Ｅ１（Ｇ＋Ｕ）＋Ｓ）の情報が送られることになる。

【００５７】このとき、２次暗号化処理部２４は、検証局端末装置３０への送信データ（２次暗号化画像データＥ２（Ｅ１（Ｇ＋Ｕ）＋Ｓ））に対するハッシュ値Ｈ２を生成および署名し、署名情報Ｓを除く電子透かしに関連する秘密情報と、２次暗号化の秘密鍵とを共に検証局端末装置３０に送る。なお、秘密情報とは、電子透かしを検出するための埋め込み位置や強度に関する情報であり、検証局端末装置３０と共有している他の暗号方式によって暗号化して送られるものである。

【００５８】また、ハッシュ値とは、一般にハッシュ関数ｈ()の出力値であり、ハッシュ関数とは衝突を起こしにくい圧縮関数をいう。ここで、衝突とは、異なる値ｘ１，ｘ２に対してｈ（ｘ１）＝ｈ（ｘ２）となることである。また、圧縮関数とは、任意のビット長のビット列をある長さのビット列に変換する関数である。したがって、ハッシュ関数とは、任意のビット長のビット列をある長さのビット列に変換する関数ｈ()で、ｈ（ｘ１）＝ｈ（ｘ２）を満たす値ｘ１，ｘ２を容易に見出せないものである。このとき、任意の値ｙからｙ＝ｈ（ｘ）を満たす値ｘを容易に見出せないので、必然的にハッシュ関数は一方向性関数となる。このハッシュ関数の具体例としては、ＭＤ（Message Digest）５やＳＨＡ（Secure Hash Algorithm）等が知られている。

【００５９】４）次に、検証局端末装置３０では、第２端末装置２０から送られてきたハッシュ値Ｈ２の署名と、そのハッシュ値Ｈ２が送信データのハッシュ値と一致することとを確認し、その確認後に２次復号処理部３１は、第２端末装置２０からの２次暗号化画像データＥ２（Ｅ１（Ｇ＋Ｕ）＋Ｓ）を復号し、そこから署名情報Ｓを抽出する。そして、電子透かし確認処理部３２で署名情報Ｓを検査し、正しければ検証情報を作成して検証局端末装置３０の署名を付ける。最後に、検証局端末装置３０は、第２端末装置２０から送信された２次暗号化

画像データＥ２（Ｅ１（Ｇ＋Ｕ）＋Ｓ）の情報とハッシュ値Ｈ２とその署名、およびそれに対する検証情報とその署名とを第１端末装置１０に送る。

【００６０】５）次に、第１端末装置１０において、第１のエンティティは、検証局端末装置３０から送られてきた検証情報とその署名とを確認し、さらに２次暗号化画像データＥ２（Ｅ１（Ｇ＋Ｕ）＋Ｓ）とハッシュ値Ｈ２とその署名とを確認する。その確認後に１次復号処理部１４は、上記２次暗号化画像データＥ２（Ｅ１（Ｇ＋Ｕ）＋Ｓ）の１次暗号化を復号してＥ２（Ｇ＋Ｕ）＋Ｄ１（Ｅ２（Ｓ））の情報を生成し、それを第２端末装置２０に送る。

【００６１】６）次に、第２端末装置２０において、２次復号処理部２５は、第１端末装置１０から送られてきたＥ２（Ｇ＋Ｕ）＋Ｄ１（Ｅ２（Ｓ））の情報の２次暗号化を復号して電子透かし付き画像データＧｗを取り出す。よって、電子透かし付き画像データＧｗは、Ｇｗ＝Ｇ＋Ｕ＋Ｄ１（Ｓ）と表わされる。これは、もとの画像データＧに対して利用者情報Ｕと１次復号の影響を受けた第２のエンティティの署名情報Ｓとが透かし情報として埋め込まれていることを示す。

【００６２】もし、第１のエンティティまたは第２のエンティティのどちらかの不正によって上記４）の過程において正しい透かし情報が検証局端末装置３０で検証されない場合、そのことが第１端末装置１０と第２端末装置２０とに知らせられる。この時点で取り引きが中止されても、第１のエンティティは代価を得られないが画像データを第２のエンティティに不正入手されず、第２のエンティティは画像データを入手できないが第１のエンティティに代価を支払うことはない。したがって、第１のエンティティおよび第２のエンティティのどちらも、利益も不利益もなく不正をする意味がない。

【００６３】すなわち、上記の電子透かし埋め込み処理を実行すれば、第１の埋込処理において第２のエンティティである代理店は、第１のエンティティであるサーバまたは著作者の原画像データＧに対して自分の署名情報Ｓを埋め込んだ電子透かし付き画像データＧｗを得ることができる。なお、第１の埋込処理における利用者情報および署名情報をそれぞれＵ１，Ｓ１とすると、代理店が得る電子透かし付き画像データＧｗは、Ｇｗ＝Ｇ＋Ｕ１＋Ｄ１（Ｓ１）となる。

【００６４】次に、第２の埋込処理において、代理店の得た電子透かし付き画像データＧｗを原画像として同様の埋め込み処理を行えば（代理店を第１のエンティティとする）、このとき第２のエンティティとなるユーザは、電子透かし付き画像データＧww＝Ｇ＋Ｕ１＋Ｄ１（Ｓ１）＋Ｕ２＋Ｄ３（Ｓ２）を得ることができる。ただし、第２の埋込処理における利用者情報および署名情報をそれぞれＵ２，Ｓ２とし、代理店が行う暗号化をＥ３（）、復号をＤ３（）で表わすものとする。

【００６５】不正コピー（不正画像）が発見された場合は、以下のような簡単な検証処理で不正者を容易に特定できる。以下に述べる検証処理も、第１の埋込処理に対応するサーバまたは著作者と代理店間の検証処理である第１の検証処理と、第２の埋込処理に対応する代理店とユーザ間の検証処理である第２の検証処理とに分けて行う。その順番は、まず第１の検証処理を行い、次に第２の検証処理を行う。

【００６６】ただし、第１の検証処理において下記の利用者情報および署名情報はＵ１，Ｓ１であり、代理店が行う暗号化および復号はＥ３（），Ｄ３（）である。また、第２の検証処理において下記の利用者情報および署名情報はＵ２，Ｓ２である。なお、ここでは上述の文献[1]、[2]と同様に画像データは透かし情報の変形および消去を受けないという仮定をおく。

【００６７】[検証処理]

１）まず第１の検証処理で、第１端末装置１０において第１のエンティティは、発見した不正画像Ｇｗ’＝Ｇ＋Ｕ’＋Ｄ１（Ｓ’）から利用者情報Ｕ’を抽出し、さらに上記不正画像Ｇｗ’を１次暗号化して署名情報Ｓ’を抽出する。ここで利用者情報Ｕ’が抽出されない場合は、第１のエンティティの不正と認定する。

【００６８】２）第１の検証処理において正しい署名情報が抽出された場合（Ｓ’＝Ｓの場合）は、第２の検証処理へと進む。第２の検証処理においても同様の処理を行い、正しい署名情報が抽出された場合は、第２のエンティティの不正と認定する。これは、正しい署名情報は第２のエンティティにしか作成できず、第１のエンティティは署名情報を知ることはできないためである。３）また、正しい署名情報が抽出されない場合（Ｓ’≠Ｓの場合）は、第１のエンティティの不正と認定する。

【００６９】この第１の実施形態による電子透かし方式では、ディジタルデータの暗号化処理および電子透かし情報の埋め込み処理を第１端末装置１０と第２端末装置２０との両方で行い、暗号処理および埋め込んだ電子透かし情報の正当性の確認を検証局端末装置３０が行っているので、第１のエンティティまたは第２のエンティティが単独で不正コピーを行ってもその不正行為を容易に確認することができ、また、不正者も簡単に検証することができる。

【００７０】また、この方式では第１の埋込処理および第２の埋込処理の各処理ごとに検証局による検査が行われるので、結託は意味を持たず、サーバまたは著作者と代理店とユーザとの何れかの結託はあり得ない。仮に結託しても、不正行為は容易に確認することができる。なお、この処理の安全性は、検証局が信頼できるということに根拠を置く。

【００７１】〔第２の実施形態〕近年、電子現金と呼ばれるネットワーク上の通貨が実現されつつある。この電子現金は、通常の現金と同様に所有者の名前が記されな

いので匿名性が実現されている。もし、匿名性が実現されない場合、商品の売り手は、電子現金から誰がどの商品を購入したかという情報を知ることができ、ユーザのプライバシーが犯されることになる。このため、上述した電子透かしによる著作者の著作権保護と同様に、ユーザのプライバシー保護の実現は重要である。

【００７２】そこで、この第２の実施形態では、購入時にはユーザの匿名性が実現され、画像の不正配布のような不正が発見されたときには、電子透かしの本来の目的である不正配布者の特定が行えるようにする。これは、例えば、図２に示すようなシステム２００により実現される。このシステム２００は、上述した第１の実施形態におけるシステム１００と同様の構成としているが、第２端末装置２０には、認証局４０からの匿名公開鍵証明書が与えられる構成としている。

【００７３】通常、署名情報を検査する公開鍵には、その正当性を証明するために認証局と呼ばれる機関による証明書が付されていることが多い。この認証局とは、公開鍵暗号方式におけるユーザの公開鍵の正当性を保証するために、ユーザの公開鍵に証明書を発行する機関を言う。すなわち、認証局は、ユーザの公開鍵やユーザに関するデータに認証局の秘密鍵で署名を施すことによって証明書を作成し、発行する。あるユーザから自分の証明書付き公開鍵を送られた他のユーザは、この証明書を認証局の公開鍵で検査することによって、公開鍵を送ってきたユーザの正当性（少なくとも、認証局によって認められたユーザであるということ）を認証する。このような認証局を運営している組織として、VeriSignやCyberTrustという企業がよく知られている。

【００７４】よって、上述した第１の実施形態で述べた第２の埋込処理中の２）の手順において代理店がユーザの契約情報を署名から確認する場合、図２の認証局４０の証明書付きの公開鍵で確認することが考えられる。しかしながら、この証明書には通常、公開鍵の所有者の名前が記されている。よってこの場合、データの購入時におけるユーザの匿名性は実現されていないことになる。

【００７５】これに対して、公開鍵とその所有者との対応を認証局４０が秘密に保持すれば、公開鍵の証明書に所有者の名前を記さないこともできる。このような匿名性を有する公開鍵の証明書を、以後「匿名公開鍵証明書」と呼び、そのような証明書付きの公開鍵を「証明書付き匿名公開鍵」と呼ぶ。そこで、ユーザは、上述した第２の埋込処理中の１）の手順において、契約情報と一緒に契約情報の署名、および署名情報Ｓを検査するための証明書付き匿名公開鍵を送れば、ユーザはディジタルデータの購入時に自分を匿名にすることができる。

【００７６】よって、代理店には利用者を特定する情報として証明書付き匿名公開鍵が渡されるが、不正コピーの発見時には、その証明書付き匿名公開鍵を認証局４０に示してその公開鍵に対応するユーザを教えてもらうことによって、ユーザを特定することができる。以上のことから、上述した第１の実施形態で述べた第２の埋込処理中の１），２）の手順と、第２の検証処理中の１）の手順とを以下のように変えることにより、ユーザのディジタルデータ購入時の匿名性と不正発見時の不正者特定との両方を実現することができる。

【００７７】以下、上記図２のシステム２００における埋め込み処理、および検証処理について具体的に説明する。

【００７８】[埋め込み処理]

１）まず、第２端末装置２０において、契約生成処理部２１は、認証局４０で発行された証明書付き匿名公開鍵と一緒に、所望の画像データを要求する契約情報をその公開鍵に対応する署名を付けて第１端末装置１０に送る。

２）次に、第１端末装置１０において、契約確認処理部１１は、第２のエンティティの公開鍵を認証局４０の公開鍵によって検査するとともに、契約情報の署名を第２のエンティティの匿名公開鍵から確認し、その確認後に、少なくとも契約情報および証明書付き匿名公開鍵の一方から利用者情報Ｕを作成する。そして、電子透かし埋め込み処理部１２により上記契約確認処理部１１で作成された利用者情報Ｕを要求された画像データＧに埋め込んだ後、１次暗号化処理部１３により１次暗号化処理Ｅ１()を行い、得られたデータを第２端末装置２０に送る。よって、第２端末装置２０には、１次暗号化画像データＥ１（Ｇ＋Ｕ）の情報が送られる。以下の３）～６）の手順は第１の実施形態で述べた手順と同様なので、ここでは重複する説明を省略する。

【００７９】[検証処理]

１）第２の検証処理で第１端末装置１０は、発見した不正画像Ｇww'から利用者情報を抽出し、さらに不正画像Ｇww'を１次暗号化して署名情報を抽出する。さらに、その抽出された利用者情報と契約情報から分かる匿名公開鍵とを認証局４０に示し、その匿名公開鍵に対応する第２のエンティティ名を聞く。ここで利用者情報が抽出されない場合は、第１のエンティティの不正と認定する。以下の２）および３）の手順は第１の実施形態で述べた手順と同様である。

【００８０】以上述べたように、第２の実施形態によれば、ユーザはディジタルデータの購入時において検証局に対しても匿名性が保つことができる。

【００８１】〔第３の実施形態〕第３の実施形態では、図１６または図１７に示したサーバまたは著作者が代理店を通してユーザにディジタルデータを配付する処理を一括して考える。以下、本発明に係る第３の実施形態を、図３を参照しながら説明する。すなわち、第３の実施形態に係る電子透かし方式は、例えば、図３に示すようなシステム３００により実施され、このシステム３００は、本発明に係る電子情報配布システムを適用したも

のでもある。

【００８２】第３の実施形態に係るシステム３００は、サーバ側の端末装置（以下、サーバ端末装置と記す）５０、代理店側の端末装置（以下、代理店端末装置と記す）６０、ユーザ側の端末装置（以下、ユーザ端末装置と記す）７０および検証局側の端末装置（以下、検証局端末装置と記す）３０を含む多数のエンティティ（図示せず）からなるネットワークシステムであり、各エンティティは、ネットワークを介して互いにディジタルデータの授受を行うようになされている。

【００８３】サーバ端末装置５０は、例えば画像データ（ディジタルデータ）が供給される１次暗号化処理部５１と、ユーザ端末装置７０および検証局端末装置３０からのデータが供給される１次復号処理部５２とを備えており、１次暗号化処理部５１の出力が代理店端末装置６０に送信されるとともに、１次復号処理部５２の出力がユーザ端末装置７０に送信されるようになされている。

【００８４】代理店端末装置６０は、ユーザ端末装置７０からのデータが供給される契約確認処理部６１と、サーバ端末装置５０の１次暗号化処理部５１の出力が供給される電子透かし埋め込み処理部６２とを備えており、電子透かし埋め込み処理部６２の出力がユーザ端末装置７０および検証局端末装置３０に送信されるようになされている。

【００８５】ユーザ端末装置７０は、代理店端末装置６０の契約確認処理部６１に対してデータを送信する契約生成処理部７１と、署名生成処理部７２と、署名生成処理部７２および代理店端末装置６０の電子透かし埋め込み処理部６２からのデータが供給される電子透かし埋め込み処理部７３と、電子透かし埋め込み処理部７３の出力が供給される２次暗号化処理部７４と、サーバ端末装置５０の１次復号処理部５２からのデータが供給される２次復号処理部７５とを備えており、２次復号処理部７５の出力が電子透かし付き画像データとして出力されるようになされている。また、２次暗号化処理部７４の出力は、サーバ端末装置５０の１次復号処理部５２および検証局端末装置３０に各々供給されるようになされている。

【００８６】検証局端末装置３０は、代理店端末装置６０の電子透かし埋め込み処理部６２およびユーザ端末装置７０の２次暗号化処理部７４の出力が供給される２次復号処理部３１と、２次復号処理部３１の出力が供給される電子透かし確認処理部３２とを備えており、電子透かし確認処理部３２の出力がサーバ端末装置５０の１次復号処理部５２に供給されるようになされている。

【００８７】以下に、上記のように構成したシステム３００の動作を説明する。なお、この図３に示されるプロトコルにおいて、方式や秘密鍵等の１次暗号に関する情報はサーバまたは著作者だけが知る情報であり、２次暗号に関する情報はユーザだけが知る情報である。ただし、これらの暗号の間には、どちらの暗号化を先に行っても復号を行うとその暗号は解かれる、という性質を持つものとする。以下では、図１７のような階層システムを対象にして説明を行うが、以下において著作者をサーバと読み替えれば、図１６のシステムに対する説明となる。

【００８８】[埋め込み処理]

１）まず、ユーザ端末装置７０において、ユーザが署名を付けて代理店端末装置６０に所望の画像データを要求する。この要求データは、契約生成処理部７１により生成された情報（ユーザの署名情報）であり、以下ではこれを契約情報と呼ぶ。代理店では、契約確認処理部６１において、受信した契約情報をユーザの署名から確認し、その確認後に画像データをサーバ端末装置５０（著作者）に要求する。これを受けてサーバ端末装置５０における１次暗号化処理部５１は、画像データＧに対して１次暗号化処理Ｅ１()を行い、得られたデータＥ１（Ｇ）を代理店端末装置６０に送る。

【００８９】２）次に、代理店端末装置６０において、契約確認処理部６１は、ユーザ端末装置７０より受信した契約情報から利用者情報Ｕを作成する。そして、電子透かし埋め込み処理部６２は、上記契約確認処理部６１で作成された利用者情報Ｕをサーバ端末装置５０から送られた１次暗号化画像データＥ１（Ｇ）に埋め込み、ユーザ端末装置７０に送る。よって、ユーザ端末装置７０には、利用者情報付きの１次暗号化画像データＥ１（Ｇ）＋Ｕの情報が送られることになる。

【００９０】このとき、代理店端末装置６０の電子透かし埋め込み処理部６２は、電子透かしに関する秘密情報を検証局端末装置３０に送る。なお、秘密情報とは、電子透かしを検出するための埋め込み位置や強度に関する情報であり、検証局端末装置３０と共有している他の暗号方式によって暗号化して送られるものである。

【００９１】３）次に、ユーザ端末装置７０において、署名生成処理部７２は、自分の秘密鍵を用いて署名情報Ｓを生成する。そして、電子透かし埋め込み処理部７３は、署名生成処理部７２で生成された署名情報Ｓを、代理店端末装置６０から送られてきた（配布された）１次暗号化画像データＥ１（Ｇ）＋Ｕに埋め込む。また、２次暗号化処理部７４は、電子透かし埋め込み処理部７３で署名情報Ｓが埋め込まれた１次暗号化画像データＥ１（Ｇ）＋Ｕ＋Ｓを２次暗号化して検証局端末装置３０に送る。よって、検証局端末装置３０には、２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ＋Ｓ）の情報が送られることになる。

【００９２】このとき、ユーザ端末装置７０の２次暗号化処理部７４は、検証局端末装置３０への送信データ（２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ＋Ｓ））に対するハッシュ値Ｈ２を生成および署名し、電子透かしに関連する秘密情報と、２次暗号化の秘密鍵とを共に

検証局端末装置３０に送る。

【００９３】４）次に、検証局端末装置３０では、ユーザ端末装置７０から送られてきたハッシュ値Ｈ２の署名と、そのハッシュ値Ｈ２が送信データのハッシュ値と一致することとを確認し、その確認後に２次復号処理部３１は、ユーザ端末装置７０からの２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ＋Ｓ）を復号し、そこから利用者情報Ｕと署名情報Ｓとを抽出する。そして、電子透かし確認処理部３２で上記利用者情報Ｕと署名情報Ｓとを検査し、正しければ検証情報を作成して検証局端末装置３０の署名を付ける。最後に、検証局端末装置３０は、ユーザ端末装置７０から送信された２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ＋Ｓ）とハッシュ値Ｈ２とその署名、およびそれに対する検証情報とその署名とをサーバ端末装置５０に送る。

【００９４】５）次に、サーバ端末装置５０において、著作者は、検証局端末装置３０から送られてきた検証情報とその署名とを確認し、さらに２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ＋Ｓ）とハッシュ値Ｈ２とその署名とを確認する。その確認後に１次復号処理部５２は、上記２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ＋Ｓ）の１次暗号化を復号してＥ２（Ｇ）＋Ｄ１（Ｅ２（Ｕ＋Ｓ））の情報を生成し、それをユーザ端末装置７０に送る。

【００９５】６）次に、ユーザ端末装置７０において、２次復号処理部７５は、サーバ端末装置５０から送られてきたＥ２（Ｇ）＋Ｄ１（Ｅ２（Ｕ＋Ｓ））の情報の２次暗号化を復号して電子透かし付き画像データＧｗを取り出す。よって、電子透かし付き画像データＧｗは、Ｇｗ＝Ｇ＋Ｄ１（Ｕ＋Ｓ）と表わされる。これは、もとの画像データＧに対して１次復号の影響を受けた利用者情報Ｕとユーザの署名情報Ｓとが透かし情報として埋め込まれていることを示す。

【００９６】もし、著作者またはユーザのどちらかの不正によって上記４）の過程において正しい透かし情報が検証局端末装置３０で検証されない場合、そのことがサーバ端末装置５０と代理店端末装置６０とユーザ端末装置７０とに知らせられる。この時点で取り引きが中止されても、誰にとっても利益も不利益もなく、不正をする意味がない。なお、不正コピー（不正画像）Ｇｗ’が発見された場合は、以下のような簡単な検証処理で不正者を容易に特定できる。ただし、ここでは上述の文献[1]、[2]と同様に、画像データは透かし情報の変形および消去を受けないという仮定をおく。

【００９７】[検証処理]

１）まず、サーバ端末装置５０において、著作者は発見した不正画像Ｇｗ’を１次暗号化して利用者情報を抽出する。ここで利用者情報が抽出されない場合は著作者の不正と認定する。

２）一方、正しい利用者情報が抽出された場合は、上記不正画像Ｇｗ’を１次暗号化したデータから署名情報を抽出する。

３）ここで、正しい署名情報が抽出された場合は、ユーザの不正と認定する。これは、正しい署名情報はユーザにしか作成できず、著作者および代理店は署名情報を知ることはできないためである。

４）また、正しい署名情報が抽出されない場合は著作者の不正と認定する。

【００９８】この第３の実施形態による電子透かし方式では、ディジタルデータの暗号化処理および電子透かし情報の埋め込み処理をサーバ端末装置５０と代理店端末装置６０とユーザ端末装置７０との三者で行い、暗号処理および埋め込んだ電子透かし情報の正当性の確認を検証局端末装置３０が行っているので、著作者、代理店またはユーザが単独で不正コピーを行ってもその不正行為を容易に確認することができ、また、不正者も簡単に検証することができる。また、この方式では著作者、代理店およびユーザの利害は相反するので結託はあり得ない。仮に結託しても、不正行為は容易に確認することができる。なお、この処理の安全性は、検証局が信頼できるということに根拠を置く。

【００９９】〔第４の実施形態〕第４の実施形態においても第３の実施形態と同様に、図１６または図１７に示したサーバまたは著作者が代理店を通してユーザにディジタルデータを渡す処理を一括して考える。以下、本発明に係る第４の実施形態を、図４を参照しながら説明する。すなわち、第４の実施形態に係る電子透かし方式は、例えば、図４に示すようなシステム４００により実施され、このシステム４００は、本発明に係る電子情報配布システムを適用したものでもある。

【０１００】第４の実施形態に係るシステム４００は、サーバ端末装置５０、代理店端末装置６０、ユーザ端末装置７０および検証局端末装置３０を含む多数のエンティティ（図示せず）からなるネットワークシステムであり、各エンティティは、ネットワークを介して互いにディジタルデータの授受を行うようになされている。

【０１０１】サーバ端末装置５０は、例えば画像データ（ディジタルデータ）が供給される１次暗号化処理部５１と、代理店端末装置６０および検証局端末装置３０からのデータが供給される１次復号処理部５２とを備えており、１次暗号化処理部５１の出力が代理店端末装置６０に送信されるとともに、１次復号処理部５２の出力がユーザ端末装置７０に送信されるようになされている。

【０１０２】代理店端末装置６０は、ユーザ端末装置７０からのデータが供給される契約確認処理部６１と、契約確認処理部６１およびサーバ端末装置５０の１次暗号化処理部５１の出力が供給される電子透かし埋め込み処理部６２と、ユーザ端末装置７０からのデータが供給される電子透かし埋め込み処理部６３とを備えており、一方の電子透かし埋め込み処理部６２の出力がユーザ端末

装置７０に送信されるとともに、他方の電子透かし埋め込み処理部６３の出力がサーバ端末装置５０および検証局端末装置３０に送信されるようになされている。

【０１０３】ユーザ端末装置７０は、代理店端末装置６０の契約確認処理部６１に対してデータを送信する契約生成処理部７１と、署名生成処理部７２と、代理店端末装置６０の電子透かし埋め込み処理部６２の出力が供給される２次暗号化処理部７４と、サーバ端末装置５０の１次復号処理部５２からのデータが供給される２次復号処理部７５とを備えており、２次復号処理部７５の出力が電子透かし付き画像データとして出力されるようになされている。また、２次暗号化処理部７４の出力は、代理店端末装置６０の電子透かし埋め込み処理部６３および検証局端末装置３０に各々供給されるようになされている。

【０１０４】検証局端末装置３０は、代理店端末装置６０の電子透かし埋め込み処理部６３およびユーザ端末装置７０の２次暗号化処理部７４の出力が供給される２次復号処理部３１と、２次復号処理部３１および代理店端末装置６０の電子透かし埋め込み処理部６３の出力が供給される電子透かし確認処理部３２とを備えており、電子透かし確認処理部３２の出力がサーバ端末装置５０の１次復号処理部５２に供給されるようになされている。

【０１０５】以下に、上記のように構成したシステム４００の動作を説明する。なお、この図４に示されるプロトコルにおいて、方式や秘密鍵等の１次暗号に関する情報はサーバまたは著作者だけが知る情報であり、２次暗号に関する情報はユーザだけが知る情報である。ただし、これらの暗号の間には、どちらの暗号化を先に行っても復号を行うとその暗号は解かれる、という性質を持つものとする。以下では、図１７のような階層システムを対象にして説明を行うが、以下において著作者をサーバと読み替えれば、図１６のシステムに対する説明となる。

【０１０６】[埋め込み処理]

１）まず、ユーザ端末装置７０において、ユーザが署名を付けて代理店端末装置６０に所望の画像データを要求する。この要求データは、契約生成処理部７１により生成された情報（ユーザの署名情報）であり、以下ではこれを契約情報と呼ぶ。代理店では、契約確認処理部６１において、受信した契約情報をユーザの署名から確認し、その確認後に画像データをサーバ端末装置５０（著作者）に要求する。これを受けてサーバ端末装置５０における１次暗号化処理部５１は、画像データＧに対して１次暗号化処理Ｅ１()を行い、得られたデータＥ１（Ｇ）を代理店端末装置６０に送る。

【０１０７】２）次に、代理店端末装置６０において、契約確認処理部６１は、ユーザ端末装置７０より受信した契約情報から利用者情報Ｕを作成する。そして、電子透かし埋め込み処理部６２は、上記契約確認処理部６１で作成された利用者情報Ｕをサーバ端末装置５０から送られた１次暗号化画像データＥ１（Ｇ）に埋め込み、ユーザ端末装置７０に送る。よって、ユーザ端末装置７０には、利用者情報付きの１次暗号化画像データＥ１（Ｇ）＋Ｕの情報が送られることになる。

【０１０８】３）次に、ユーザ端末装置７０において、２次暗号化処理部７４は、代理店端末装置６０より送られた１次暗号化画像データＥ１（Ｇ）＋Ｕを２次暗号化し、得られた画像データＥ２（Ｅ１（Ｇ）＋Ｕ）の情報を代理店端末装置６０に送る。このとき、署名生成処理部７２では、ユーザが自分にしか作成できない署名情報Ｓを生成し、２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ）と共に代理店端末装置６０に送る。また、２次暗号化処理部７４は、２次暗号化の秘密鍵を検証局端末装置３０に送る。

【０１０９】４）次に、代理店端末装置６０において、電子透かし埋め込み処理部６３は、ユーザ端末装置７０から送られてきた２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ）に対して同じくユーザ端末装置７０から送られてきた署名情報Ｓを埋め込み、検証局端末装置３０に送る。よって、検証局端末装置３０には、署名情報付きの２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ）＋Ｓの情報が送られることになる。

【０１１０】このとき、代理店端末装置６０では、検証局端末装置３０への送信データ（２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ）＋Ｓ）に対するハッシュ値Ｈ２を生成および署名し、電子透かしに関連する秘密情報と共に検証局端末装置３０に送る。なお、秘密情報とは、電子透かしを検出するための埋め込み位置や強度に関する情報であり、検証局端末装置３０と共有している他の暗号方式によって暗号化して送られるものである。

【０１１１】５）次に、検証局端末装置３０では、代理店端末装置６０から送られてきたハッシュ値Ｈ２の署名と、そのハッシュ値Ｈ２が送信データのハッシュ値と一致することとを確認し、その確認後に、電子透かし確認処理部３２で代理店端末装置６０からの２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ）＋Ｓより署名情報Ｓを抽出するとともに、２次復号処理部３１で上記２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ）＋Ｓの２次暗号化を復号し、そこから利用者情報Ｕを抽出する。

【０１１２】そして、電子透かし確認処理部３２は、上記抽出した利用者情報Ｕと署名情報Ｓとを検査し、正しければ検証情報を作成して検証局端末装置３０の署名を付ける。最後に、検証局端末装置３０は、代理店端末装置６０から送信された２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ）＋Ｓとハッシュ値Ｈ２とその署名、およびそれに対する検証情報とその署名とをサーバ端末装置５０に送る。

【０１１３】６）次に、サーバ端末装置５０において、著作者は、検証局端末装置３０から送られてきた検証情

報とその署名とを確認し、さらに２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ）＋Ｓとハッシュ値Ｈ２とその署名とを確認する。その確認後に１次復号処理部５２は、上記２次暗号化画像データＥ２（Ｅ１（Ｇ）＋Ｕ）＋Ｓの１次暗号化を復号してＥ２（Ｇ）＋Ｄ１（Ｅ２（Ｕ）＋Ｓ）の情報を生成し、それをユーザ端末装置７０に送る。

【０１１４】７）次に、ユーザ端末装置７０において、２次復号処理部７５は、サーバ端末装置５０から送られてきたＥ２（Ｇ）＋Ｄ１（Ｅ２（Ｕ）＋Ｓ）の情報の２次暗号化を復号して電子透かし付き画像データＧｗを取り出す。よって、電子透かし付き画像データＧｗは、Ｇｗ＝Ｇ＋Ｄ１（Ｕ＋Ｄ２（Ｓ））と表わされる。これは、もとの画像データＧに対して１次復号の影響を受けた利用者情報Ｕと更に２次復号の影響も受けた署名情報Ｓとが透かし情報として埋め込まれていることを示す。

【０１１５】もし、著作者またはユーザのどちらかの不正によって上記５）の過程において正しい透かし情報が検証局端末装置３０で検証されない場合、そのことがサーバ端末装置５０と代理店端末装置６０とユーザ端末装置７０とに知らせられる。この時点で取り引きが中止されても、誰にとっても利益も不利益もなく、不正をする意味がない。なお、不正コピー（不正画像）Ｇｗ’が発見された場合は、以下のような簡単な検証処理で不正者を容易に特定できる。ただし、ここでは上述の文献[1]、[2]と同様に、画像データは透かし情報の変形および消去を受けないという仮定をおく。

【０１１６】[検証処理]

１）まず、サーバ端末装置５０において、著作者は発見した不正画像Ｇｗ’を１次暗号化して利用者情報Ｕ’を抽出する。ここで利用者情報Ｕ’が抽出されない場合は著作者の不正と認定する。

２）一方、正しい利用者情報が抽出された場合、サーバ端末装置５０は、１次暗号化された画像データＧｗ’と利用者情報Ｕ’とを検証局端末装置３０に示し、検査を要求する。検証局端末装置３０は、１次暗号された画像データＧｗ’を２次暗号化し（この暗号化機能は不図示）、署名情報を抽出する。

３）ここで、正しい署名情報が抽出された場合はユーザの不正と認定する。

４）また、正しい署名情報が抽出されない場合は著作者の不正と認定する。

【０１１７】この第４の実施形態による電子透かし方式でも、ディジタルデータの暗号化処理および電子透かし情報の埋め込み処理をサーバ端末装置５０と代理店端末装置６０とユーザ端末装置７０との三者で行い、暗号処理および埋め込んだ電子透かし情報の正当性の確認を検証局端末装置３０が行っているので、著作者、代理店またはユーザが単独で不正コピーを行ってもその不正行為を容易に確認することができ、また、不正者も簡単に検証することができる。また、この方式では著作者、代理店およびユーザの利害は相反するので結託はあり得ない。仮に結託しても、不正行為は容易に確認することができる。なお、この処理の安全性は、検証局が信頼できるということに根拠を置く。

【０１１８】〔第５の実施形態〕第５の実施形態は、図３に示した第３の実施形態において、第２の実施形態と同様にディジタルデータの購入時にはユーザの匿名性が実現され、画像の不正配布のような不正が発見されたときには不正配布者の特定が行えるようにしたものである。これは、例えば、図５に示すようなシステム５００により実現される。このシステム５００は、上述した第３の実施形態におけるシステム３００と同様の構成としているが、ユーザ端末装置７０には、認証局４０からの匿名公開鍵証明書が与えられる構成としている。

【０１１９】本実施形態でも第２の実施形態と同様に、公開鍵とその所有者との対応を認証局４０が秘密に保持することにより、公開鍵の証明書に所有者の名前を記さないことができるようにしている。そこで、ユーザは、上述した第３の実施形態における埋め込み処理中の１）の手順において、契約情報と一緒に契約情報の署名、および署名情報Ｓを検査するための証明書付き匿名公開鍵を送れば、ユーザはディジタルデータの購入時に自分を匿名にすることができる。

【０１２０】よって、代理店には利用者を特定する情報として証明書付き匿名公開鍵が渡されるが、不正コピーの発見時には、その証明書付き匿名公開鍵を認証局４０に示してその公開鍵に対応するユーザを教えてもらうことによって、ユーザを特定することができる。以上のことから、上述した第３の実施形態で述べた埋め込み処理中の１）の手順と、検証処理中の１）の手順とを以下のように変えることにより、ユーザのディジタルデータ購入時の匿名性と不正発見時の不正者特定との両方を実現することができる。

【０１２１】なお、第４の実施形態を示す図４のシステム４００中のユーザ端末装置７０に対して認証局４０を設け、上述した第４の実施形態で述べた埋め込み処理中の１）の手順と、検証処理中の１）の手順とを以下のように変えることによっても、ユーザのディジタルデータ購入時の匿名性と不正発見時の不正者特定との両方を実現することができる。

【０１２２】以下、上記図５のシステム５００における埋め込み処理、および検証処理について具体的に説明する。

【０１２３】[埋め込み処理]

１）まず、ユーザ端末装置７０において、契約生成処理部７１は、認証局４０で発行された証明書付き匿名公開鍵と一緒に、所望の画像データを要求する契約情報をその公開鍵に対応する署名を付けて代理店端末装置６０に送る。代理店では、契約確認処理部６１において、受信

した契約情報を匿名公開鍵から確認し、その確認後に画像データを著作者に要求する。これを受けてサーバ端末装置５０における１次暗号化処理部５１は、画像データＧに対して１次暗号化処理Ｅ１()を行い、得られたデータＥ１（Ｇ）を代理店端末装置６０に送る。以下の２）～６）の手順は第３の実施形態で述べた手順と同様なので、ここでは重複する説明を省略する。

【０１２４】[検証処理]

１）サーバ端末装置５０において１次暗号各処理部５１は、発見した不正画像Ｇｗ’を１次暗号化して利用者情報を抽出する。そして、その抽出した利用者情報と契約情報から分かる匿名公開鍵とを認証局４０に示し、その匿名公開鍵に対応するユーザ名を聞く。ここで利用者情報が抽出されない場合は、著作者の不正と認定する。以下の２）～４）の手順は第３の実施形態で述べた手順と同様である。

【０１２５】以上述べたように、第５の実施形態によれば、ユーザはディジタルデータの購入時において検証局に対しても匿名性が保つことができる。

【０１２６】上述の第１～第５の実施形態に示した画像データ、および電子透かし情報の埋め込み処理によって得られるハッシュ値を含む種々のデータは、以下のような画像フォーマットで格納することができる。例えば、下記の一般的な画像フォーマットでは、各段階で送付される画像データを画像データ部に格納し、それに対応するハッシュ値やその署名などを画像ヘッダ部に格納することができる。また、最終的にユーザが保存しておく必要があるハッシュ値およびその署名や、２次暗号の鍵等を画像ヘッダ部に、電子透かし付き画像データを画像データ部に格納しておくことができる。

【０１２７】一方、下記に示すFlashPixTMファイルフォーマットでは、上記のようなハッシュ値やその署名を含む一般的な画像フォーマットを各階層のデータとして格納することができる。また、ハッシュ値やその署名などは、属性情報としてプロパティセットの中に格納しておくこともできる。

【０１２８】まず、一般的な画像フォーマットについて説明する。一般的な画像フォーマットでは、図６に示すように、画像ファイルは画像ヘッダ部と画像データ部とに分けられる。

【０１２９】一般的に画像ヘッダ部には、その画像ファイルから画像データを読み取るときに必要な情報や、画像の内容を説明する付帯的な情報が格納される。図６の例では、その画像フォーマット名を示す画像フォーマット識別子、ファイルサイズ、画像の幅・高さ・深さ、圧縮の有無、解像度、画像データの格納位置へのオフセット、カラーパレットのサイズなどの情報が格納されている。一方、画像データ部は、画像データを順次格納している部分である。このような画像フォーマットの代表的な例としては、Microsoft 社のＢＭＰフォーマットや Compuserve社のＧＩＦフォーマットなどが広く普及している。

【０１３０】次に、FlashPixTMファイルフォーマットについて具体的に説明する。以後説明するFlashPixTM（FlashPixは米国Eastman Kodak 社の登録商標）ファイルフォーマットでは、上記画像ヘッダ部に格納されていた画像属性情報および画像データ部に格納されていた画像データを、更に構造化してファイル内に格納する。この構造化した画像ファイルを、図７および図８に示す。ファイル内の各プロパティやデータには、ＭＳ－ＤＯＳのディレクトリとファイルに相当する、ストレージとストリームによってアクセスする。上記図７、図８において、影付き部分がストレージで、影なし部分がストリームである。画像データや画像属性情報はストリーム部分に格納される。

【０１３１】図７において、画像データは異なる解像度で階層化されており、それぞれの解像度の画像をSubimageと呼び、Resolution０，１，…，ｎで示してある。各解像度の画像に対して、その画像データを読み出すために必要な情報がSubimage Header に、また画像データがSubimage data に格納される。プロパティセットとは、属性情報をその使用目的や内容に応じて分類して定義したものであり、Summary info. Property Set、Image info. Property Set、Image Content Property Set、Extention list property Set がある。

【０１３２】[各プロパティセットの説明]Summary info. Property Setは、FlashPix特有のものではなく、Microsoft 社のストラクチャードストレージでは必須のプロパティセットで、そのファイルのタイトル・題名・著者・サムネール画像等を格納する。また、Comp Obj. Streamには記憶部（Strage）に関する一般的な情報が格納される。

【０１３３】Image Content Property Setは、画像データの格納方法を記述する属性である（図９参照）。この属性には、画像データの階層数、最大解像度の画像の幅や高さ、それぞれの解像度の画像についての幅、高さ、色の構成、あるいはＪＰＥＧ圧縮を用いる際の量子化テーブル・ハフマンテーブルの定義などを記述する。Extention list property Set は、上記FlashPixの基本仕様に含まれない情報を追加する際に使用する領域である。さらに、ICC Profile の部分には、ＩＣＣ（International Color Consortium）において規定される色空間変換のための変換プロファイルが記述される。

【０１３４】また、Image info. Property Setは、画像データを使用する際に利用できる様々な情報、例えば、その画像がどのようにして取り込まれ、どのように利用可能であるかの下記のような情報を格納する。

・ディジタルデータの取り込み方法／あるいは生成方法に関する情報

・著作権に関する情報

・画像の内容（画像中の人物、場所など）に関する情報
・撮影に使われたカメラに関する情報
・撮影時のカメラのセッティング（露出、シャッタースピード、焦点距離、フラッシュ使用の有無など）の情報
・ディジタルカメラ特有の解像度やモザイクフィルタに関する情報
・フィルムのメーカ名、製品名、種類（ネガ／ポジ、カラー／白黒）等の情報
・オリジナルが書物や印刷物である場合の種類やサイズに関する情報
・スキャン画像の場合、使用したスキャナやソフト、操作した人に関する情報

【０１３５】図８のFlashPix Image View Objectは、画像を表示する際に用いるビューイングパラメータと画像データとを合わせて格納する画像ファイルである。ビューイングパラメータとは、画像の回転、拡大／縮小、移動、色変換、フィルタリングの処理を画像表示の際に適応するために記憶しておく処理係数のセットである。この図８において、Global info. Property Set の部分には、ロックされている属性リストが記述されており、例えば、最大画像のインデックスや最大変更項目のインデックス、最終修正者の情報などが記述される。

【０１３６】また、同図において、Source/Result FlashPix Image Object は、FlashPix画像データの実体であり、Source FlashPix Image Objectは必須で、Result FlashPix Image Objectはオプションである。Source FlashPix Image Objectはオリジナルの画像データを、Result FlashPix Image Objectはビューイングパラメータを使って画像処理した結果の画像データをそれぞれ格納する。

【０１３７】また、Source/Result desc. Property Setは、上記画像データの識別のためのプロパティセットであり、画像ＩＤ、変更禁止のプロパティセット、最終更新日時等を格納する。Transform Property Setは、画像の回転、拡大／縮小、移動のためのAffine変換係数、色変換マトリクス、コントラスト調整値、フィルタリング係数を格納している。

【０１３８】次に、画像データの取り扱いについて説明する。ここでは、複数のタイルに分割された複数の解像度の画像を含む画像フォーマットを例に挙げて説明する。図１０に、解像度の異なる複数の画像から構成される画像ファイルの例を示す。この図１０において、最大解像度の画像は列×行がＸ０×Ｙ０で構成されており、その次に解像度の大きい画像はＸ０／２×Ｙ０／２であり、それ以降順次、列・行ともに１／２ずつ縮小し、列・行ともに６４画素以下あるいは互いに等しくなるまで縮小されていく。

【０１３９】このように画像データを階層化した結果、画像の属性情報として「１つの画像ファイル中の階層数」や、それぞれの階層の画像に対して、一般的な画像フォーマットの項で説明したヘッダ情報と画像データとが必要となる（図６参照）。１つの画像ファイル中の階層の数や最大解像度の画像の幅、高さ、あるいはそれぞれの解像度の画像の幅、高さ、色構成、圧縮方式等に関する情報は、上記ImageContent Property Set中に記述される（図９参照）。

【０１４０】さらに、各解像度のレイヤの画像は、図１１に示すように６４画素×６４画素でなるタイル毎に分割されている。画像の左上部から順次６４画素×６４画素のタイルに分割をすると、画像によっては右端および下端のタイルの一部に空白が生ずる場合がある。この場合は、それぞれ最右端画像または最下端画像を繰り返し挿入することで、６４画素×６４画素を構築する。

【０１４１】FlashPixTMでは、それぞれのタイル中の画像データをＪＰＥＧ圧縮、シングルカラー、非圧縮のいずれかの方法で格納する。ＪＰＥＧ圧縮は、ISO/IEC JTC1/SC29 により国際標準化された画像圧縮方式であり、方式自体の説明はここでは割愛する。また、シングルカラーとは、上記１つのタイルがすべて同じ色て構成されている場合にのみ、個々の画素の値を記録することなく、そのタイルの色を１色で表現する方式である。この方法は特に、コンピュータグラフィックスにより生成された画像で有効である。

【０１４２】このようにタイル分割された画像データは、例えば図７のSubimage data ストリーム中に格納され、タイルの総数、個々のタイルのサイズ、データの開始位置、圧縮方法はすべてSubimage Header に格納されている（図１２参照）。

【０１４３】〔その他の実施形態〕以上に述べた第１～第５の実施形態において、透かし情報の埋め込みは、種々の手法によって実現できるが、例えば、「清水，沼尾，森本（日本ＩＢＭ）：“ピクセルブロックによる静止画像データハイディング”，情報処理学会第５３回全国大会，1N-11，平成８年９月」の文献や、「I. J. Cox, J. Kilian, T. Leighton and T. shamoon(ＮＥＣ)：“Sucure Spread Spectrum Watermarking for Multimedia,”ＮＥＣ Reserch Instiure Technical Report 95-10.」の文献に示されるような公知の埋め込み手法によって実現できる。

【０１４４】また、１次暗号，２次暗号として用いられる暗号方式も種々の方式によって実現できるが、例えばビットの配置を暗号鍵に応じて換えるといった暗号方式によって実現できる。また、全ての送信データにハッシュ値とその署名を付けて送ることもできる。さらに、１次暗号と２次暗号は、透かし情報の埋め込み処理において互いの情報を知らせないために用いられるが、第三者からの通信路上での盗聴および改ざんを防ぐために、別にＤＥＳ（Data Encryption Standard）等の暗号やハッシュ関数等を用いても良い。

【０１４５】また、上述の第１～第５の実施形態におい

て、不正配布の検出は第１のエンティティ（サーバまたは著作者）が行っているが、１次暗号または２次暗号に関する秘密鍵を知らなくても電子透かしの抽出手段さえ持っていれば、誰にでも不正配布および不正配布の利用者情報を知ることができる。その後、不正配布発見を第１のエンティティ側に知らせて検証処理を始めさせれば良いので、不正配布の発見者は第１のエンティティに限定されない。

【０１４６】また、第１のエンティティまたは代理店は、利用者情報Ｕだけでなく、必要に応じて著作権情報やその画像データの配布状況に関する情報等の他の情報を画像データに埋め込むこともできる。また、第１のエンティティで秘密の情報を埋め込みたい場合は、１次暗号化の後に埋め込み処理を行えば、署名情報と同様に１次暗号の影響を受けた情報を埋め込むことができる。さらに、利用者情報Ｕは、必ず１次暗号化の前にある必要はなく、１次暗号化の後に埋め込んでもよい（この場合、利用者情報Ｕの検出は、第１のエンティティまたは１次暗号の秘密鍵を知る者のみが行える）。

【０１４７】また、第２のエンティティが共通のプリンタや端末等を用いるユーザである場合、第２のエンティティの署名情報および２次暗号は、プリンタや共通端末の署名情報や暗号方式を含む場合がある。また、第１のエンティティからの１次暗号化情報は、第２のエンティティからの契約情報による依頼がなくても、ネットワークやＣＤ－ＲＯＭ等によって広く配布されていても良い。また、第２のエンティティの署名情報Ｓは、公開鍵暗号方式によって生成されなくても良く、ユーザが契約情報等で定めた情報（暗証番号のような情報）等でも良い。

【０１４８】また、米国では４０ビット以上の暗号を用いる場合、暗号の悪用を防ぐために暗号鍵を管理する鍵管理局を必要とする。そこで、検証局に鍵管理局を兼ねさせることも可能である。よって、検証局が２次暗号の鍵をあらかじめ管理している場合には、不正画像の監視も検証局が行えば、上述の検証処理１）～３）は検証局が単独で行うことができる。第１のエンティティの１次暗号の鍵は、同じ検証局によって管理されていてもよいし、他の鍵管理局によって管理されていてもよい。また、第１のエンティティや第２のエンティティの鍵は、鍵管理局が生成して配布してもよい。

【０１４９】また、代理店は１つであるとは限らず、階層的に構成されていても良い。このとき、代理店の行う処理は階層中の担当代理店が代表して行っても良いし、代理店間で上記のプロトコルを行い、責任を明らかにするようにしても良い。また、図１７のように代理店が１つの場合は、代理店に関する利用者情報Ｕ１の埋め込みを省略することができる。

【０１５０】また、著作者は要求された後に画像データＧの１次暗号情報Ｅ１（Ｇ）を代理店に送ることになっているが、１次暗号化画像データＥ１（Ｇ）をあらかじめ代理店に送るようにしても良い。また、第３の実施形態以降の代理店は暗号Ｅ３()および復号Ｄ３()を持たないが、著作者から最初にデータを送られた後、暗号Ｅ３()によって暗号化し、最後に著作者にデータを送る前に復号Ｄ３()によって復号しても良い。

【０１５１】

【発明の効果】上述の説明から明らかなように、本発明の電子透かし方式および電子情報配布システムによれば、データに対する暗号処理および電子透かし埋め込み処理を複数の手段またはエンティティで分散して行い、上記複数の手段またはエンティティで行われた上記暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を、上記複数の手段またはエンティティとは別の手段またはエンティティで検証するようにしたので、階層的に構成されたネットワークにおいてデータを不正にコピーして配布を行った際にその不正行為および不正行為者を確実に認識することができ、これによって不正を確実に防止することが可能となり、データの不正配布に関して安全なシステムを実現することができる。さらに、このシステムによってユーザの匿名性や暗号の悪用を防ぐ鍵管理局への応用も容易に実現することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態を示した電子透かしシステムを説明するための図である。

【図２】本発明の第２の実施形態を示した電子透かしシステムを説明するための図である。

【図３】本発明の第３の実施形態を示した電子透かしシステムを説明するための図である。

【図４】本発明の第４の実施形態を示した電子透かしシステムを説明するための図である。

【図５】本発明の第５の実施形態を示した電子透かしシステムを説明するための図である。

【図６】一般的な画像フォーマットを示す図である。

【図７】FlashPixTMファイルフォーマットの例を示す図である。

【図８】FlashPixTMファイルフォーマットの例を示す図である。

【図９】FlashPixTMファイルフォーマットのImage Content Property Setに格納される属性情報を示す図である。

【図１０】それぞれ解像度の異なる複数の画像から構成される画像ファイルの例を示す図である。

【図１１】各解像度のレイヤの画像のタイル分割の様子を示す図である。

【図１２】タイル分割された画像データに関する属性情報を示す図である。

【図１３】従来の電子透かしシステムを説明するための図である。

【図１４】図１３に示す方式を改良した従来の電子透かしシステムを説明するための図である。

【図１５】図１４に示す方式を改良した従来の電子透かしシステムを説明するための図である。

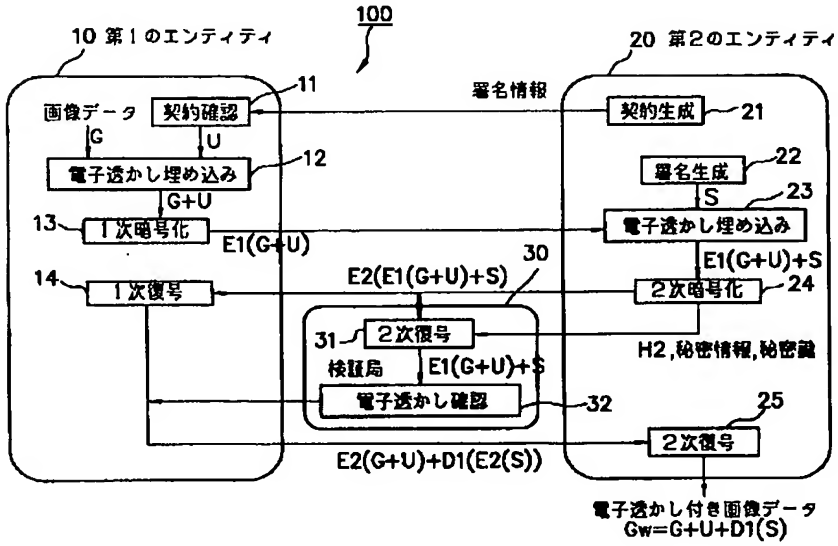
【図１６】階層的に構成されたデータ配付システムの一例を示す図である。

【図１７】階層的に構成されたデータ配付システムの他の例を示す図である。

【符号の説明】

１０　第１のエンティティ側の端末装置
１１　契約確認処理部
１２　電子透かし埋め込み処理部
１３　１次暗号化処理部
１４　１次復号処理部
２０　第２のエンティティ側の端末装置
２１　契約生成処理部
２２　署名生成処理部
２３　電子透かし埋め込み処理部
２４　２次暗号化処理部
２５　２次復号処理部
３０　検証局端末装置
＊３１　２次復号処理部
３２　電子透かし確認処理部
４０　認証局端末装置
５０　サーバ端末装置
５１　１次暗号化処理部
５２　１次復号処理部
６０　代理店端末装置
６１　契約生成処理部
６２　電子透かし埋め込み処理部
６３　電子透かし埋め込み処理部
７０　ユーザ端末装置
７１　契約生成処理部
７２　署名生成処理部
７３　電子透かし埋め込み処理部
７４　２次暗号化処理部
７５　２次復号処理部
１００　電子情報配布システム
２００　電子情報配布システム
３００　電子情報配布システム
４００　電子情報配布システム
＊　５００　電子情報配布システム

【図１】



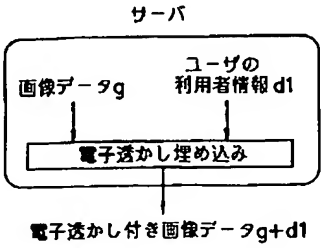
【図６】

画像ヘッダ部	画像フォーマット識別子
	ファイルサイズ
	X方向ピクセル数（幅）
	Y方向ピクセル数（高さ）
	深さ方向サイズ
	圧縮の有無
	解像度
	ビットマップへのオフセット
	カラーパレットサイズ
画像データ部	ビットマップ

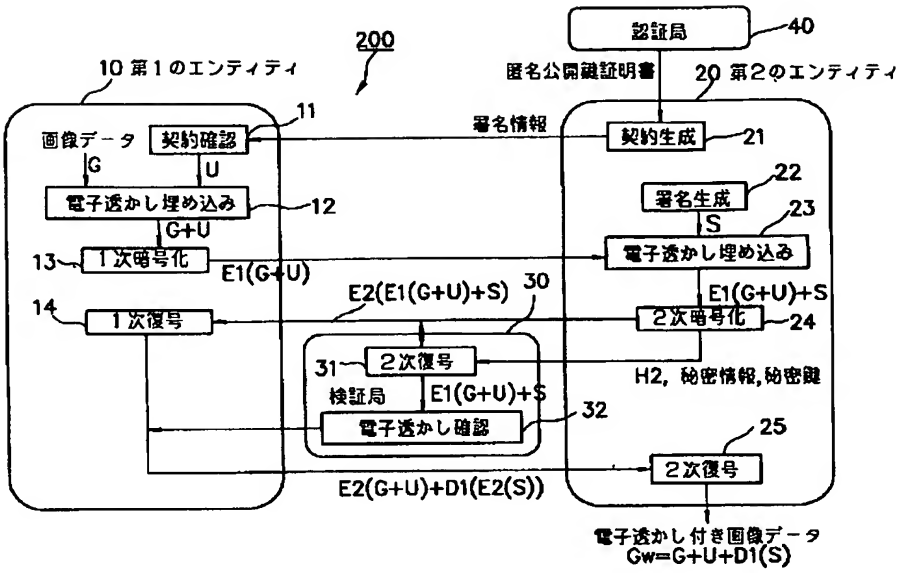
【図１２】

フィールド名	長さ	バイト
画像の幅	4	4−7
画像の高さ	4	8−11
タイルの総数	4	12−15
タイルの幅	4	16−19
タイルの高さ	4	20−23

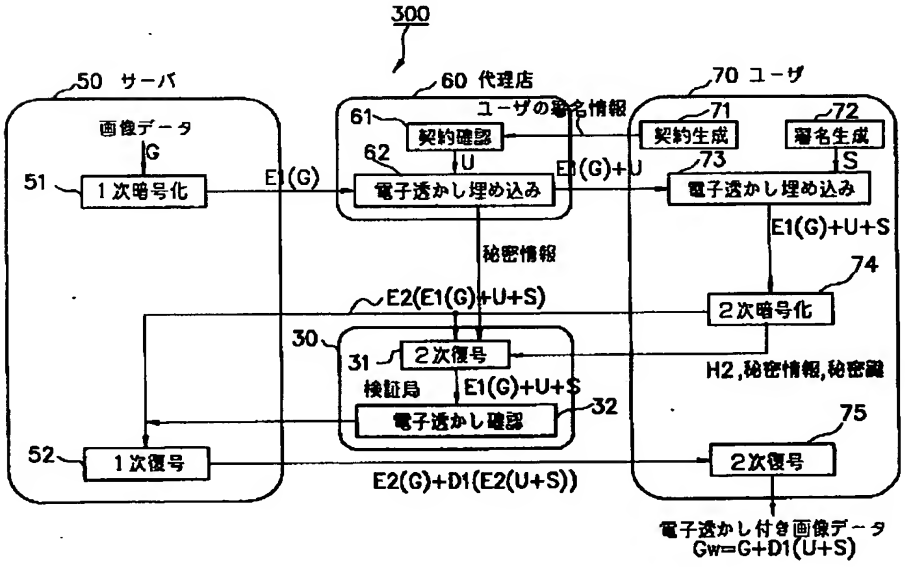
【図１３】



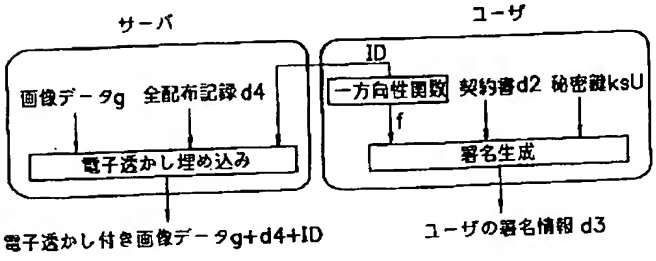
【図２】


200
認証局
40
10 第１のエンティティ
匿名公開鍵証明書
20 第２のエンティティ
画像データ
契約確認
11
署名情報
契約生成
21
G
U
電子透かし埋め込み
12
署名生成
22
G+U
S
23
13
１次暗号化
E1(G+U)
電子透かし埋め込み
E2(E1(G+U)+S)
30
E1(G+U)+S
14
１次復号
２次暗号化
24
31
２次復号
H2, 秘密情報,秘密鍵
検証局
E1(G+U)+S
32
電子透かし確認
25
２次復号
E2(G+U)+D1(E2(S))
電子透かし付き画像データ
Gw=G+U+D1(S)

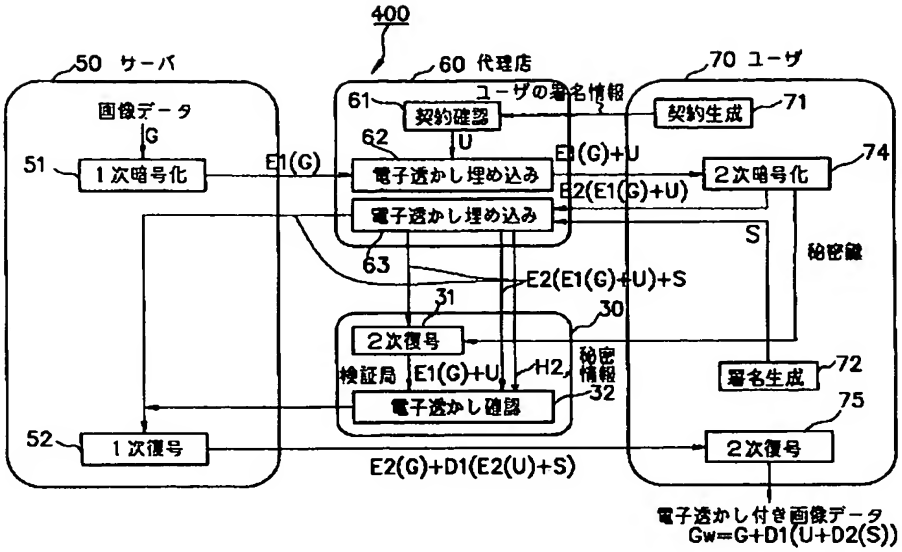
【図３】


300
50 サーバ
60 代理店
70 ユーザ
ユーザの署名情報
画像データ
61
契約確認
71
契約生成
72
署名生成
G
62
U
S
51
１次暗号化
E1(G)
電子透かし埋め込み
E1(G)+U
73
電子透かし埋め込み
E1(G)+U+S
秘密情報
74
E2(E1(G)+U+S)
２次暗号化
30
31
２次復号
H2,秘密情報,秘密鍵
検証局
E1(G)+U+S
32
電子透かし確認
75
52
１次復号
２次復号
E2(G)+D1(E2(U+S))
電子透かし付き画像データ
Gw=G+D1(U+S)

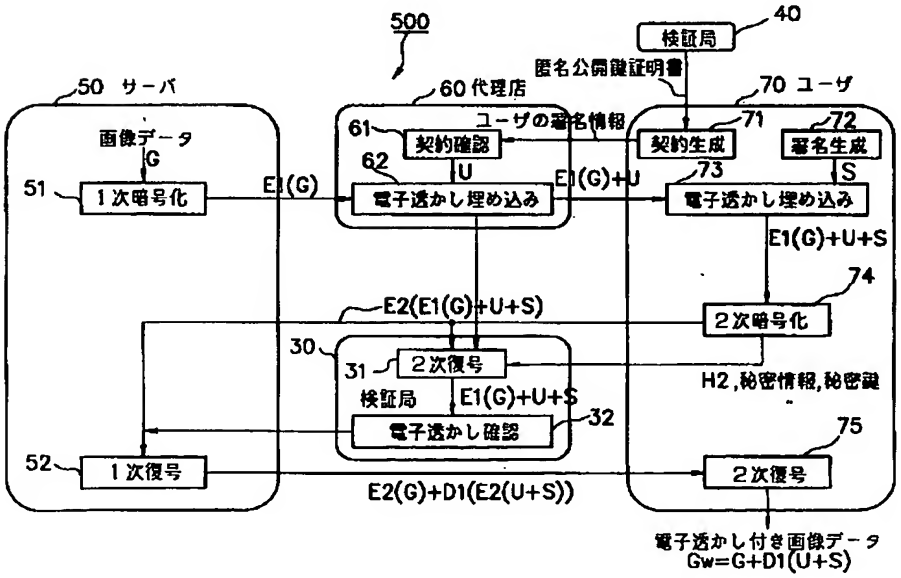
【図１４】


サーバ
ユーザ
ID
画像データg
全配布記録d4
一方向性関数
契約書d2
秘密鍵ksU
f
電子透かし埋め込み
署名生成
電子透かし付き画像データg+d4+ID
ユーザの署名情報 d3

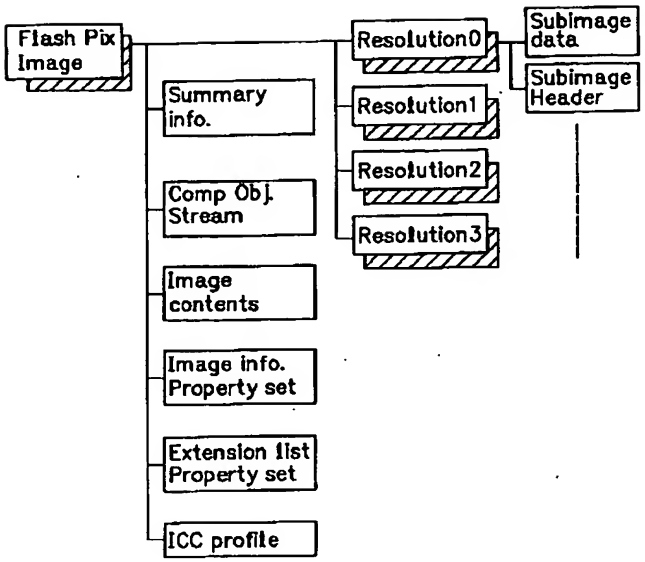
【図４】


400
50 サーバ
60 代理店
70 ユーザ
画像データ
G
51
1次暗号化
E1(G)
61
契約確認
ユーザの署名情報
契約生成
71
62
U
電子透かし埋め込み
E3(G)+U
2次暗号化
74
E2(E1(G)+U)
電子透かし埋め込み
S
秘密鍵
63
E2(E1(G)+U)+S
31
30
2次復号
検証局
E1(G)+U
H2,
秘密情報
32
電子透かし確認
署名生成
72
75
52
1次復号
2次復号
E2(G)+D1(E2(U)+S)
電子透かし付き画像データ
Gw=G+D1(U+D2(S))

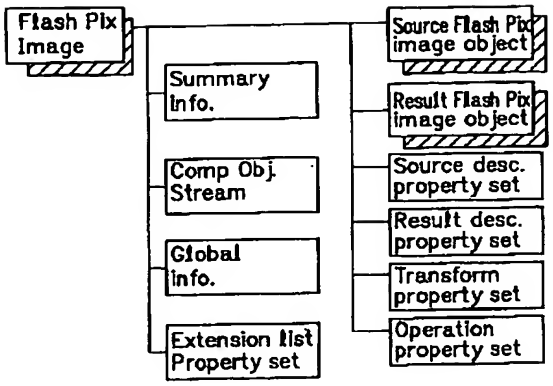
【図５】


500
検証局
40
匿名公開鍵証明書
50 サーバ
60 代理店
70 ユーザ
画像データ
G
61
契約確認
ユーザの署名情報
契約生成
71
72
署名生成
51
1次暗号化
E1(G)
62
U
電子透かし埋め込み
E1(G)+U
73
S
電子透かし埋め込み
E1(G)+U+S
74
E2(E1(G)+U+S)
2次暗号化
30
31
2次復号
H2,秘密情報,秘密鍵
検証局
E1(G)+U+S
32
電子透かし確認
75
52
1次復号
2次復号
E2(G)+D1(E2(U+S))
電子透かし付き画像データ
Gw=G+D1(U+S)

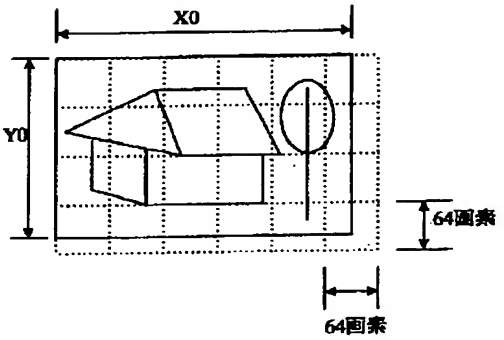
【図７】



【図８】



【図１１】



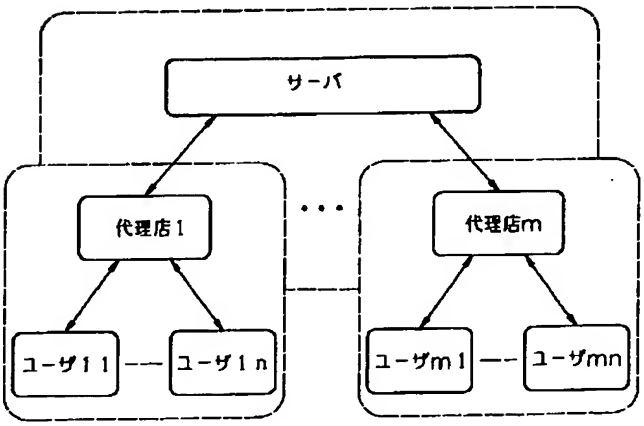
【図９】

プロパティ名	IDコード	タイプ
画像データの階層数	0x01000000	VT_UI4
最大解像度の画像の幅	0x01000002	VT_UI4
最大解像度の画像の高さ	0x01000003	VT_UI4
初期表示の高さ	0x01000004	VT_R4
初期表示の幅	0x01000005	VT_R4

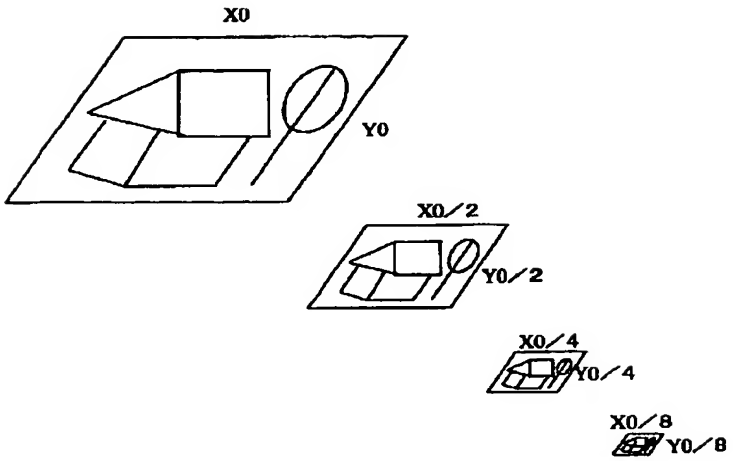
プロパティ名	IDコード	タイプ
各解像度の画像の幅	0x02ii0000	VT_UI4
各解像度の画像の高さ	0x02ii0001	VT_UI4
各解像度の画像の色	0x02ii0002	VT_BLOB
各解像度の画像を数値で表わしたフォーマット	0x02ii0003	VT_UI4 | VT_VECTOR

プロパティ名	IDコード	タイプ
JPEGテーブル	0x03ii0001	VT_BLOB
最大JPEGテーブルのインデックス	0x03000002	VT_UI4

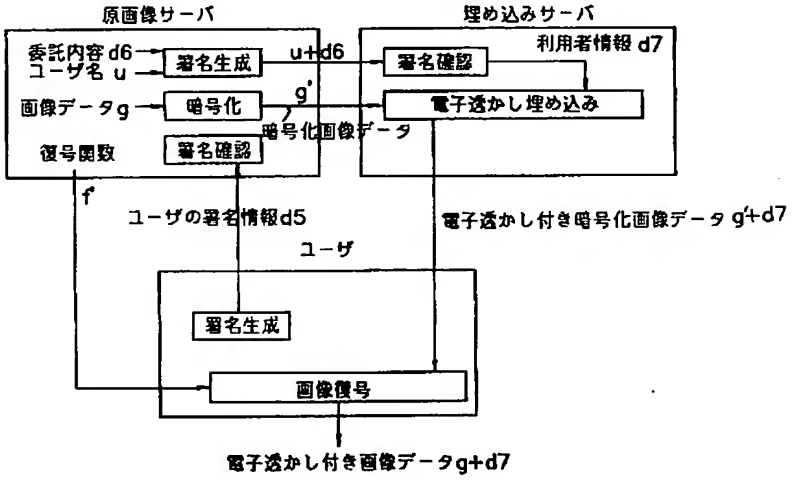
【図１６】



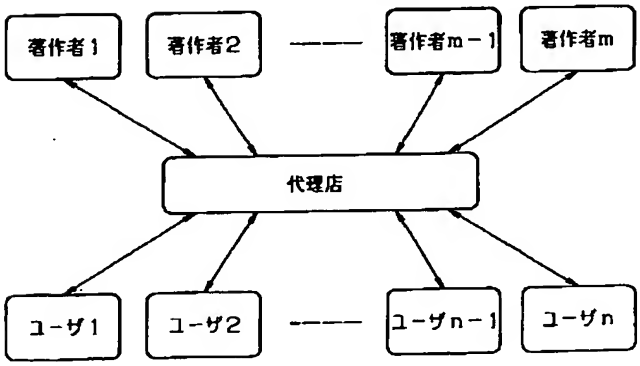
【図１０】


X0
Y0
X0／2
Y0／2
X0／4
Y0／4
X0／8
Y0／8

【図１５】


原画像サーバ
埋め込みサーバ
委託内容 d6
ユーザ名 u
署名生成
u+d6
署名確認
利用者情報 d7
画像データg
暗号化
g'
電子透かし埋め込み
暗号化画像データ
復号関数
署名確認
f
ユーザの署名情報d5
電子透かし付き暗号化画像データ g'+d7
ユーザ
署名生成
画像復号
電子透かし付き画像データg+d7

【図１７】


著作者1
著作者2
著作者m－1
著作者m
代理店
ユーザ1
ユーザ2
ユーザn－1
ユーザn

フロントページの続き

(51) Int. Cl.[6]	識別記号	F I
H０４N 7/081		